Encryption in Education

Educational Institutions at High Risk for Costly Data Breaches

The Ponemon Institute estimates that on average, organizations of all types face a 26% probability of a data breach involving 10,000 or more lost or stolen records – and educational institutions are increasingly becoming targets. In fact, the education vertical tied for 2nd place in Symantec’s 2016 Internet Security Threat Report for sub-sectors with the highest number of security breach incidents. This unfortunate state means that one out of every four schools – possibly more – will have at least one significant data breach while adding the costs of encryption-based prevention tactics can be a burden to an already strained budget, they’re a small fraction of the impact that a breach will have on your school. Are you financially prepared for that eventuality?

Breaches in data security happen more often than you may realize and incidents at educational institutes are on the rise. More than 280,000 financial and personal data records have been compromised during the first five months of 2016 at the University of California, Berkeley; the University of Central Florida; and at Southern New Hampshire University (an online university) - and these are just the ones we know about.

Many organizations that report breaches remain unsure just how many records are compromised, and many more are unaware that data has been compromised and therefore fail to report. Hence, the total is likely much higher. For example, in April of 2015, Auburn University admitted a significant security breach involving 360,000 people whose social security numbers were exposed online publicly over a three-year period. These individuals were not even registered or enrolled students of the university but were either applicants or prospective students. The alarming issue here is that the breach was active for three years before the university detected it, and then the school’s network had to be shut down for three full days, significantly affecting ongoing operations.

Security breaches are expensive. In 2016 the average cost of a data breach in the US was $7.01 million per incident or on average, $211 per lost or stolen record, and these costs are even higher for educational organizations. According to the Ponemon Institute, the expense of data breaches varies by industry and educational organizations have the second highest average cost at $220 per lost or stolen record. This equates to potential expenses to a school of over $7.3 million for each incident (using Ponemon’s average number of breached records per incident of 29,611) - many organizations experience more than one data breach.

What would the impact be to your school should any significant amount of personally identifiable information (PII) be compromised? Does your school have the human resources needed to manage auditors, press, and affected individuals? Does your school have the budget and funds readily available to pay regulatory and civil fines, plus personal retribution? How would daily operations be affected if your organization was no longer allowed to accept credit card payments? Finally, what type of intangible damage would be done to your school’s reputation, and how would that affect future enrollment, staff recruiting, grant applications, and research projects?
Schools Struggle to Protect Large Volumes of Sensitive Data

Educational institutions of all sizes routinely handle multiple types of personally-identifiable data, including social security numbers, credit card numbers, driver’s license numbers, passport numbers, addresses, phone numbers, bank/debit account numbers, medical information, and other sensitive data which can potentially be stolen. In addition, due to their focus on research, these organizations may also have access to confidential government and/or business intelligence data regarding trade, scientific, or military secrets.

Personally identifiable information (PII) requires special handling to adhere to compliance regulations, however not all higher educational institutions are adequately protecting it. In fact, only 76% of higher educational organizations having institutional policies restricting access to PII, whereas 71% simply try to avoid storing PII data. Of the PII data that is stored, much of it is not encrypted. SANS estimates that on average only 54% of higher educational institutions encrypt PII in transit, and a mere 48% encrypt PII at rest. Organizations that do not encrypt PII data at rest and in transit are at significantly higher risk for security breaches.

Schools Face Complex Data Security Regulatory Mandates

Academic organizations must adhere to numerous, overlapping, privacy-related regulations when it comes to safeguarding the personally identifiable information they manage. The top six regulations that impact educational institutions include:

1. The Family Educational Rights and Privacy Act (FERPA) deals with the protection of student records and applies only to educational institutions that receive government funding.

2. The Health Insurance Portability and Accountability Act (HIPAA) regulates the protection of medically related PII data and may apply to schools which provide healthcare services and engage in HIPAA covered transactions such as billing health plans.

3. The Health Information Technology for Economic and Clinical Health Act (HITECH) promotes the adoption and meaningful use of electronic health records (EHR) and supporting health information technology, and protects educational institutions from penalties from lost or stolen data if they can prove the data was encrypted before the breach.

4. The Children's Online Privacy Protection Act (COPPA) enables parents to have control over what information is collected online from their children under age 13 and applies to school online properties and the vendors with whom they contract to manage them.

5. The Payment Card Industry Data Security Standard (PCI DSS) impacts an organization's payment systems and applies to schools which use third-party vendors to process credit card transactions.

6. State data breach notification laws, such as California's S. B. 1394, requires educational entities to notify individuals of security breaches of information involving personally identifiable information.

Depending on the type of organization and its funding, educational institutions may also be subject to Graham-Leach-Bliley (GLB), FISMA, Sarbanes-Oxley (SOX), and ITAR regulations.

This range of compliance requirements can strain the limited resources of institutions already constrained by budget, resources, and staff. In particular, staffing and employee retention are especially problematic because most higher education organizations don’t have the budget to attract and retain experienced IT security analysts. To help address these gaps, improve compliance, and reduce risk, educational organizations should consider security tools such as encryption to protect data in transit, at rest, or stored on removable media.
The Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law passed in 1974 that protects the privacy of student education records and that bars the disclosure of personally identifiable data in student records including name, student identification number, Social Security Number, or a portion thereof in a personally identifiable manner, without the parent's or eligible student's written consent. An eligible student is a student who is 18 years old or attending a postsecondary institution at any age. For example, it is a violation of FERPA (or the “Buckley Amendment”) to publicly post on the Web (or by any other medium) final course grades using the last four digits of a student's social security number. The FERPA law applies to all schools that receive funds under any applicable program administered by the U.S. Department of Education – from practitioners of early learning to those developing systems across the education continuum (P-20), including both the schools and their contractors. Most private schools are not subject to FERPA because these schools typically do not receive federal money.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a set of regulations to help protect the privacy and security of particular health information. The U.S. Department of Health and Human Services (HHS) published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule.

The Security Rule within HIPAA does not explicitly require encryption, but “[e]ncryption is deemed “addressable.” The Security Rule goes on to state that entities should perform a risk assessment and implement encryption if the evaluation indicates that encryption would be a “reasonable and appropriate” safeguard. If an entity decides not to encrypt electronic protected health information (ePHI), it has to document and justify that decision and then implement an “equivalent alternative measure.”

This requirement spotlights the juncture at which industry-standard best practices play such an important role. Similarly, when determining the ideal method of encryption, the U.S. Department of Health & Human Services turns to the National Institute of Standards and Technology for recommended encryption practices. HHS and NIST have both produced robust documentation for adhering to HIPAA’s Security Rule. NIST Special Publication 800-111 takes a broad approach to encryption on end-user devices, but in a nutshell it states that when there’s even a remote possibility of risk, encryption needs to be in place, and FIPS 140-2, which incorporates the Advanced Encryption Standard (AES) into its protocols, is an ideal choice.

Many organizations leverage the U.S. government's Federal Information Processing Standard Publication 140-2 (FIPS 140-2) to aid in their pursuit of compliance. Specifically, FIPS 140-2 helps education entities ensure that PII is “rendered unusable, unreadable, or indecipherable to unauthorized individuals.” A device that meets FIPS 140-2 requirements possesses a cryptographic erase function that “leverages the encryption of target data by enabling sanitization of the target data's encryption key, leaving only the ciphertext remaining on the media, effectively sanitizing the data.”

FIPS 140-2 features four levels of increasing security. Level 1 requires that a solution use an approved algorithm or security function; the device itself requires no physical security. Level 2 adds the requirement for some form of physical security that can present evidence of an unauthorized access attempt, such as a tamper-proof seal. A Level 3 solution goes even further by requiring a countermeasure that thwarts access, use, or modification of the cryptographic module if the solution itself detects a physical breach. Level 4 takes FIPS 140-2 protection to its pinnacle by detecting environmental variations (such as voltage and/or temperature) outside of a specified range and taking action to destroy cryptographic keys when it detects a breach.
FERPA / HIPAA Interaction and Exceptions

FERPA and HIPAA do not always work together seamlessly, which causes some complexity. The HIPAA Privacy Rule typically does not apply to an elementary or secondary school because the school either (1) is not a HIPAA covered entity or (2) is a HIPAA covered entity but maintains health information only on students in records that are by definition “education records” under FERPA and are therefore not subject to the HIPAA Privacy Rule. Even though an elementary or secondary school may employ school nurses, physicians, psychologists, or other health care providers, the school is not generally a HIPAA-covered entity because the providers do not engage in any of the HIPAA covered transactions, such as billing a health plan electronically for their services.

For schools such as universities that do employ a health care provider that conducts one or more covered transactions electronically, such as electronically transmitting health care claims to a health plan for payment, the school is considered a HIPAA covered entity and must comply with the HIPAA Transactions and Code Sets and Identifier Rules with respect to such transactions. However, even in this case, many schools would not be required to comply with the HIPAA Privacy Rule because the school maintains health information only in student health records that are “education records” under FERPA and, thus, not “protected health information” under HIPAA. Since student health information in education records is protected by FERPA, the HIPAA Privacy Rule excludes such information from its coverage.

For example, if a public high school employs a health care provider that bills Medicaid electronically for services provided to a student, the school is a HIPAA covered entity and would be subject to the HIPAA requirements concerning transactions. However, if the school's provider maintains health information only in what are education records under FERPA, the school is not required to comply with the HIPAA Privacy Rule. Rather, the school would have to comply with FERPA's privacy requirements with respect to its education records, including the requirement to obtain parental consent (34 CFR § 99.30) in order to disclose to Medicaid billing information about a service provided to a student.

When FERPA does not apply, then the HIPAA exemption for records covered by FERPA does not apply. While this means that HIPAA may potentially apply, it is possible that no privacy law applies. HIPAA does not actually apply to every health care record held by schools, even when FERPA does not apply. HIPAA only applies to certain types of businesses which are defined strictly under HIPAA as “covered entities.” Covered entities are typically healthcare providers who bill for services, as for example, hospitals, doctors, etc. This point is a very important one to clarify before a student receives health care, including mental health counseling, at a private school.

Health Information Technology for Economic and Clinical Health (HITECH) Act

Perhaps the best reason to encrypt data came with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Passed in 2009, the HITECH Act protects healthcare entities from serious penalties for any lost or stolen data provided that the data was encrypted before the breach. Considering examples such as two stolen laptops resulting in a $3 million fine (a fine that could have been avoided under HITECH), the comparative cost of data encryption seems trivial. In other words, schools and the vendors with whom they do business simply can't afford not to encrypt all data at rest.

Encryption must extend beyond laptops and backup drives. Communicating or sending data over the Internet needs Transport Layer Security (TLS), a protocol for transmitting data over a network, and AES encryption. When an employee accesses a business's local network, a secure VPN connection is essential when ePHI is involved. Also, before putting a handful of student files on a flash drive for transfer between systems or offices, a harmless and innocent act in most situations, it is imperative to realize that a self-encrypting flash drive that also meets FIPS 140-2 requirements is the best option to avoid HIPAA violations.
Payment Card Industry Data Security Standard (PCI DSS)

For schools with internal billing departments or schools, which handle and transmit credit card data for American Express, Discover, JCB, MasterCard, or Visa, the Payment Card Industry’s Data Security Standard defines how to protect sensitive cardholder data and the penalties for failing to do so adequately. The PCI DSS applies to ANY organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.

Many schools use credit card payment systems in dining halls, bookstores, university-based hotel/conference centers, vending machines, or via web-based payment systems for tuition, athletic tickets, or alumni donations. Because it can be challenging to comply with PCI DSS, many educational institutions try to run such money collection systems over separate secure networks. Either they effectively segment the business functions of their organizations that deal with credit card payments or they offload this business to a third-party vendor. It is important to note that merely using a third-party company does not exclude a school from PCI DSS compliance. It may cut down on your risk exposure and consequently reduce the effort required to validate compliance, but it does not mean that you can ignore the PCI DSS.

If a school is not PCI-DSS compliant, it risks losing its ability to process credit card payments, getting audited, and/or fined. The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this penalty along until it eventually hits your school or your third party vendor, who will then pass it on to your school. Furthermore, the bank will also most likely either terminate your relationship or increase your transaction fees. PCI DSS penalties are not openly discussed nor widely publicized, but they can be catastrophic – especially for small, private schools. It is important to be familiar with your merchant account agreement, which should outline your exposure.

A recent survey by Diamond Mind Payment Solutions for Schools, noted that 45% of independent schools are not entirely PCI-compliant or do not know if they are compliant. Many do not even know what it would take to achieve or maintain compliance. Many school officers do not realize that PCI compliance requires an annual self-assessment and a quarterly vulnerability scan. Larger schools are more likely to report being compliant (65%) than smaller schools (47%); however, many have not yet created a culture of PCI awareness. Regardless of whether organizations manage credit card billing systems internally or through third parties, a good faith effort to achieve PCI may make penalties less severe or less likely in the event of a breach of credit card data.
Children's Online Privacy Protection Rule (“COPPA”)

Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998 to allow parents to have control over what information is collected online from children under the age of 13. COPPA imposes certain requirements on operators of websites or online services directed towards children under 13 years of age. The law also prohibits a website owner, online service, or operator from “knowingly collecting information from children under the age of 13 unless the operator obtains parental consent and allows parents to review their children’s information and restrict its further use.”

The law is regulated by the Federal Trade Commission, not the US Department of Education, and applies to any operators of websites, online services including web-based testing, programs or “apps” that collect, use, or disclose children's personal information, whether at home or at school. The personal information that it applies to can include the child’s name, email, phone number, or other persistent unique identifier, as well as information about parents, friends, and other persons. It is important to note that COPPA only applies to personal information collected online from children; it does not cover information collected from adults that may pertain to children.

Many school districts work with third party vendors to offer online programs solely for the benefit of their students and the school system (e.g. homework help lines, online research and organizational tools, web-based testing services etc.) In these cases, the schools may act as the parent’s agent and can consent to the collection of kids’ information on the parent’s behalf. However, the school’s ability to consent for the parent is limited to the educational context - an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose. Unfortunately, many schools fail to engage in proper due diligence in reviewing third-party privacy and data-security policies, and inadvertently authorize data collection and data-mining practices that parents find unacceptable.

Student data may be protected under state law, too. For example, California's Student Online Personal Information Protection Act, or SOPIPA, prohibits operators of online educational services from selling student data and using such information to target advertising to students or to “amass a profile” on students for a non-educational purpose. The law also requires online service providers to maintain adequate security procedures and to delete student information at the request of a school or district. States such as Oklahoma, Idaho, and Arizona require educators to include express provisions in contracts with private vendors to safeguard privacy and security or to prohibit secondary uses of student data without parental consent.

State Data Breach Notification Laws

Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have all enacted legislation like the California Security Breach Information Act (SB-1386) requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information. While there may be some slight variations dependent on each state's data breach notification law definitions, these data breach notification laws typically have provisions covering:

- Who must comply with the law (e.g., public/private schools, businesses, government entities, etc.)?
- How is “personal information” defined (e.g., name combined with SSN, driver's license or state ID, account numbers, etc.)?
- What constitutes a breach (e.g., unauthorized disclosure or access to data)?
- What are the requirements for notice (e.g., timing or method of notice, who must be notified)?
- What are the exemptions (e.g., for encrypted information)?
Real Risk

Today, encryption is a staple of the professional world. Virtually every industry that deals with personal and/or sensitive data relies on encryption to protect that data. Service providers that don't encrypt sensitive data put themselves at risk for stiff government penalties, fines, lawsuits, and more. Educational organizations and vendors that do business with them are arguably the most targeted for malicious data breaches because student information contains everything that thieves require to steal a person's identity and/or to engage in other illicit activities. With compromised education data in hand, cybercriminals have virtually free rein to make profit, inflict damage, and ruin lives.

The first step to avoiding these expensive, potentially crippling fines and other expenses associated with a breach is to pursue regulatory compliance. Regulatory compliance entails much more than simply password-protecting an office's workstations. It requires using encryption to protect data-at-rest when stored on school systems or removable media device. Indeed, data at rest that is outside the school's firewall (or "in the wild") is the top source of security breaches. According to a Ponemon's 2015 study, 96% of respondents reported a security incident involving a lost or stolen device. Education provider and associated third-party vendors must safely store data to meet compliance requirements.

Chasing Compliance: How Regulations and Encryption Fit Together

Encryption is terrific...in theory. Data stays protected, and confidential information remains locked away from the wrong eyes. In reality, though, compliance costs money, whether from purchasing hardware and software, hiring a consultant, both, or possibly more. In some instances, a particular regulation will mandate encryption in clear, unmistakable terms; failure to comply with these terms implies a violation of the law. Other times, rules may be vague about requiring encryption, leaving a gray area for businesses to decipher. For example, a regulation may dictate protection for sensitive and/or personal data without explicitly stipulating protection via encryption. Obviously, these situations are less than ideal.

When the law isn't straightforward, security experts can provide clarity if and when a consensus gives way to commonly accepted best practices. The term isn't exclusive to regulations and encryption, but it can nonetheless help guide education providers that encounter nebulous compliance verbiage. Following industry best practices will keep a business protected in times when the letter of the law proves hard to decipher. Sometimes even the government will come to educators' aid with published best practices guidance, although the availability of such documents within a given niche or application can vary widely.

The Human Factor

Educational institutions can reasonably protect themselves against known threats. For instance, they can set up firewalls to thwart incoming attacks and use virtual private networks (VPNs) and secure communication protocols, such as HTTPS, to keep data secure while in transit. However, in many cases, an entity's weakest link is its employees.

In fact, the 2015 Ponemon study indicates that respondents worry more about employee negligence (51%) than any other security threat. That's ahead of cyber attackers (35%), system failures (19%), and identity thieves (a mere 5%). Note that negligent employees aren't the same as disgruntled types, which the report classifies as "malicious insiders." Only 19% of respondents listed these employees as a chief concern.

The biggest threat is well-meaning but inattentive employees. They're the reason laptops containing treasure troves of data disappear. Since accidents and theft do happen with all too frequent predictability, responsible enterprises would be playing Russian roulette by not taking appropriate precautions (Ponemon's 2010 paper "The Billion Dollar Lost Laptop Problem" pegs the number at 7.12% across all surveyed organizations).Equipping portable devices with self-encrypting drives is one obvious step, but educational institutions should go further, particularly with at-rest data on removable storage. One might assume that a portable hard drive or USB flash drive will never be left unattended, but that's precisely the kind of employee wishful thinking and negligence that leads to breaches. Education providers must address this potential weakness.
Be Smart. Encrypt Data. Be compliant.

Cybercrime is rising, and educational institutions are high-profile targets. Unfortunately, many educational organizations are not using any encryption technology even though encryption is a mainstay security control that is required by regulations and policies. This practice must change if schools are to protect sensitive data and avoid penalties.

Adhering to data security requirements is a process, not a single step. There are many rules to follow, and a "one size fits all" approach does not work. With tight budgets and limited resources, it’s no wonder that schools are struggling to meet compliance requirements for a plethora of regulatory mandates.

Protecting sensitive data is more crucial now than ever. If your educational organization has questions about securing PPI for its students and staff, a proper risk assessment should be the first step to achieving and/or maintaining compliance. Members of the P-20 community can also contact the Privacy Technical Assistance Center and ask for guidance on privacy, confidentiality and data security.

Encryption and Security in Brief

Before learning how to protect data, it’s useful to know a little more about the data itself — specifically where it resides. For our purposes, data exists in the following three "states": at rest, in transit, and in use. Data at rest refers to data located in persistent storage, such as a hard drive. This could be as simple as a saved document or image. Data in transit is any data sent or received across a network. Downloading a file from the Internet or transferring a file between two computers on a local area network are both cases of data in transit. Data in use is a little trickier, but it essentially means any data that a computer’s CPU is actively processing or data temporarily stored within a system’s RAM.

Encryption is a deep, complicated subject that many experts devote their lives to mastering, but having a rudimentary grasp of the key terms and concepts will help healthcare organizations better understand what it takes to be compliant. Ideally, sensitive data should be secure enough that unauthorized parties can’t even access or obtain it. Even if data falls into their hands, though, they definitely shouldn’t be able to read it. That’s where encryption comes in.

Encryption transforms data to make it unreadable without authorized access. In this case, authorized access comes in the form of a decryption key, which is fairly self-explanatory. When the right people have the key, they can read your encrypted data; the wrong people who don’t have the key cannot.

Many encryption methods exist, as do different instances when encryption is necessary. Encrypting data stored on a hard drive is one example, while accessing a business’s network remotely over a virtual private network is another. Unfortunately, when it comes to compliance, there’s no universal standard for encrypting data. The regulations that govern how each industry handles data may not dictate the same encryption requirements.

People with a passing familiarity with encryption may have heard of 128-bit, 192-bit, or 256-bit encryption. This refers to the "size" of the key, in bits, necessary to decrypt data. A 128-bit key corresponds to a total of 2^128 possible keys; a 256-bit key represents 2^256 possibilities. Generally, a larger key requires more time to crack via brute force methods (where an attacker uses a computer, or multiple computers, to "guess" the key). Security experts agree that it would take modern computers billions of years to brute-force a 128-bit key. Radical advancements in computing technology (quantum computing, for example) would be necessary to break 256-bit encryption.

Of all the encryption methods, AES (Advanced Encryption Standard) receives the lion’s share of attention, and for good reason. The NSA uses AES to encrypt data, which ought to be proof enough of its security. AES can use 128-bit, 192-bit, or 256-bit keys and thus far has been extremely resistant to attempts at exploiting potential weaknesses. Several cryptographers have tried to break AES, but none have succeeded.

If there’s a downside to AES, it would be in the computational cost of its operation. For many years, most digital encryption on computers was performed “in software,” where the system’s CPU performed all of the necessary encrypt/decrypt operations. This work proved exceptionally cumbersome for general purpose processors and could bring a lower-end system to its knees. Only relatively recently have Intel’s AES New Instructions (AES-NI) and other innovations integrated specific encryption acceleration silicon into CPUs (thus running “in hardware”) and made the burden of encryption computation negligible. This also applies to the encryption of external drives, including flash drives. Somewhere, a component crunch those encryption processes, and if there’s no dedicated acceleration behind the work, other applications running on the system may suffer.

In addition to protecting data via encryption, it’s important to authenticate both data and communications (i.e., transmitted files and messages) to ensure that the data received matches the data sent. Verifying data arrived from true and trusted sources is another key aspect of maintaining security, which is why security professionals recommend cryptographic hashing. A hash is a number produced from a string of text that acts like a digital fingerprint. When someone sends a message, for example, they can generate a hash and include it with the message. The recipient of the message can then create a hash of the received message and compare it with the original hash. If the two match, the message’s authenticity is confirmed. Spoofing a hash is virtually impossible, so this tactic offers one way to ensure files and messages weren’t tampered with.

Encryption can — and should — happen in a variety of ways in a variety of situations. Windows BitLocker drive encryption is an example of one essentially free solution in the consumer space. Other times, certain hardware may be handy for encrypting data without the need for separate software. Such “self-encrypting” hardware options exist for large hard drives as well as portable flash drives. Web traffic can be encrypted using SSL (Secure Socket Layer), and the list goes on. Simply put, if desired, diligent users can keep their data encrypted wherever it goes.