Data Security and Management Training: Best Practice Considerations

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of longitudinal data systems. More PTAC information is available on http://nces.ed.gov/programs/ptac.

Purpose

Data security and data management are becoming increasingly prominent concerns as technology becomes more integral to the management of education records and education data systems. Data breaches jeopardize the confidentiality of student, parent, and staff data and result in significant financial investment in victim compensation programs and new security strategies. As education entities prudently develop and implement more powerful electronic information management systems, security training programs become a high-level priority across the nation. As such, education leaders should recognize the importance of expanding and enhancing security training for all data users, which is the best strategy for ensuring that a major threat to data security in education organizations—uninformed users—is proactively addressed before more breaches occur.

Key Training Concepts to Follow

While the terms "awareness" and "training" are sometimes used synonymously, they are actually distinct concepts that are both integral parts of an effective data security program. Awareness is typically defined as the ability to perceive or be conscious of a condition or event—and raising awareness about threats to data security is an initial goal of a comprehensive security program. The audiences for such efforts to raise awareness are often passive recipients of information, rather than interactive participants in an instructional exchange.

In contrast, training is more formal instruction about a topic (like data security) and participants should be actively engaged in exercises designed to help them apply the concepts covered in the training program. In addition to improving awareness about data management and security, training has a goal of building the knowledge and real-world skills needed to help participants do their jobs in a way that will not compromise the organization's IT and data security.

Best practice concepts that should be addressed in a security program include:

- **Awareness first, and then training.** It is tempting to jump right to training activities when implementing a security training program. However, experienced trainers understand that it is wise to first adequately prepare the target audience. Each person in an organization must understand why security is important both to them and the organization. Real world examples that are directly related to common work-associated tasks help participants see the risks facing the organization as well as the damage that can be done if security best practices (as defined in policies, standards, and guidelines) are not followed. Once awareness has been raised, employees, contractors, volunteers and other school officials can better understand why they should participate in security training. Because training, regardless of its delivery method, typically interrupts their normal job of running or supporting business operations, a key effect of raising awareness about security issues is a more engaged employee who is willing to listen and learn when training is conducted.
- **Make sure all employees are trained.** By definition, a thorough training program targets all new and current employees, as well as contract workers, temporary workers, and even volunteers. At a minimum, any member of the staff, regardless of role, who has access to personal identifiable information (PII), should be trained to protect data confidentiality and preserve system security.
- **Integrate data security training within the context of broader employee education efforts.** Incorporating data security training into an organization's overarching employee education program ensures that courses get evaluated and refreshed periodically, and that program effectiveness is regularly monitored.
- **Develop role-based training courses.** Everyone needs training, but not everyone needs the same training. Training should be tailored to reflect a user's job responsibilities, the volume of data handled, and the sensitivity of the data that an employee can access. An effective training program often includes core content that is delivered to all staff as well as tailored elements for different employee job categories, tiers, and responsibilities. Good role-based training frequently includes exercises that challenge employees to think about how they might handle situations and scenarios that are likely to arise in their current positions.
- **Incorporate breach detection and escalation in training.** In spite of even the best security training, data breaches may still occur—making it critical to train employees to recognize a potential security breach and how to escalate this information to key personnel who are designated first responders.
- **Include data security messages in all employee communications channels.** To keep privacy and security at the forefront of activities, engage in ongoing communication with employees about data security via newsletters, emails, login reminders, and other internal channels.
- **Create a culture of security in the organization.** To be truly effective, training and education should be part of the culture rather than just the required act of "taking training" and signing an acknowledgement that time was spent in a seat during the training session. Senior leaders in the organizational hierarchy must demonstrate their commitment to protecting data, securing data

systems, and training their staff to do the same.

Security Training Content

Encouraging awareness about data and IT security issues and developing a properly trained staff requires that many content areas be addressed through a comprehensive training program. When developing a security program it will be helpful to include the following essential categories:

- Risk assessment including the identification of system threats and vulnerabilities.
- Physical security (e.g., locked doors and windows), desktop security (e.g., password protected computers, mobile device security (e.g., no sensitive data on easily misplaced storage media), and network security (e.g., secure data exchange).
- Access controls including how to password protect files, encrypt transmissions and files, and authenticate users.
- Good practices related to the use of email, software/applications, and the internet.
- Phishing, hoaxes, malware, viruses, worms, spyware.
- Remote access to data and systems.
- Data backup and disaster recovery.
- Data security breach notification protocols.
- Directions for viewing written data security procedures and principles, and providing a forum to answer questions about such guidance as needed to ensure compliance.

Training Delivery Methods

Differing training goals, learning styles, participant skills, user roles, employee locations, and budgets might call for different training delivery options. Regardless of the delivery method, it's important to confirm that everyone participates. Even one employee who is unaware of the importance of data management and security and how his or her actions affect security weakens overall system security—after all, a chain is still only as strong as its weakest link.

There are three commonly used methods for delivering the security awareness message and more comprehensive data security training: on demand, virtual, and onsite.

- **On Demand Training** offers a self-paced learning environment in which participants experience a course delivered by an industry-expert or in-house trainer via a video or other previously developed mechanism (e.g., a flash tutorial). Employees can complete exercises at their own pace and location as long as they have access to a computer and the internet. On demand delivery is a good way for most distributed organizations to reach all employees.
- **Virtual Classroom Training** is delivered at specific times via web conferencing by an instructor

and provides employees with remote access to classroom systems in which they can complete virtual activities and tutorials. Because a virtual classroom offers instruction with a live (albeit virtual) instructor, this delivery method enables participants to have their questions answered and comments addressed in real-time.

- **Onsite Training** allows organizations to have an audience-appropriate training delivered at their own facility. Employees can be trained in a manner that is customized to the unique settings and circumstances of the organization, their job responsibilities, and the actual network and operational requirements of their technology environment. Some organizations reserve onsite training for more in-depth role-based training of key staff groups.

Audiences for Training

Training programs can and should be customized to the unique needs and circumstances of the organization, operational nuances, and job responsibilities. As trainers assemble content for training purposes, it will become evident that some information is universal in application, while other components of the curriculum are more appropriate for specific positions and roles.

Experienced trainers often develop levels or tiers of training. Level 1, for example, might focus on the universally important education and training topics, and be delivered to all training participants. Additional training levels might then be needed when more specialized knowledge and skills are necessary to carry out operations and responsibilities, such as when management and supervisory staff need more focused training because of their involvement in compliance functions. High-level training may also be developed for the information systems staff who need to apply guidelines and policies when administering their technology responsibilities. Under these scenarios, Level 2 training might include those items that are particular to a role or responsibility and would be aligned closely with the need-to-know parameters identified by job type.

Glossary

Access Controls limit entry to information system resources to authorized users, programs, processes, or other systems. Components of an access control system include, for example, physical access (e.g., locks on doors to a server room), authentication systems that verify the identity of a user or client machine attempting to log into a system, and file encryption that makes data unreadable to anyone who does not possess the cipher key or encryption algorithm.

Data Breach is the intentional or unintentional release of secure information to an untrusted environment.

Data Security is the means of ensuring that data are kept safe from corruption and that access to it is suitably controlled. The primary goal of any information and technology security system is to protect information and system equipment without unnecessarily limiting access to authorized users and functions.

Education Records include those records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.3.

Family Educational Rights and Privacy Act is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Personally Identifiable Information (PII) refers to information, such student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR §99.3, for a complete definition of PII specific to education data and for examples of education data elements that can be considered PII.

Risk Assessment is the process of identifying: (1) all assets an organization possesses, (2) all potential threats to those assets, (3) all points of vulnerability to those threats, (4) the probability of potential threats being realized, and (5) the cost estimates of potential losses. Risk assessment enables an organization to at least consider the range of potential threats and vulnerabilities it faces, and is the first step in effectively securing an information and technology system.