DATA BREACH POLICIES

PRESENTED BY COLLEEN YENSER, PRSBO

WHAT'S A DATA BREACH

- A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
- Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

EXAMPLES

- Grade Distributions by Teacher were published in the local newspaper
  - After report cards were completed for the current marking period, a principal received a copy of the grade distributions by teacher. He was so thrilled about how great the kids were performing that he gave a copy to his friend who is a local journalist. The grade distributions were published in the next edition of the town newspaper.

EXAMPLES

- Financial Information System Demonstration with "Demo" Data
  - Vendor met with a school district to demonstrate their system that a neighboring district was using. Demo data was a copy of the "real" data from the neighboring school district.

EXAMPLES

- Keylogger software was unknowingly installed on a business official staff's laptop
  - Targeted attack where malware installed a Keylogger on the business staff member's laptop that conducted all wire transfers. After a period of monitoring by the attacker, they distracted the business office member and transferred a LOT of funds to unauthorized bank account.
  - Malware found on Financial Information System servers

QUICK TIPS ON WHAT TO DO

WHAT TO DO?

- Before you have a breach…
  1. Build a District Breach Response Plan
  2. Conduct a Breach Simulation
     - http://ptac.ed.gov/

WHAT TO DO?

- Actual Breach
  1. Mitigate the Breach
     - Device(s) Off the Network
  2. Preserve the Evidence for Specialists
  3. Contact Appropriate Authorities
     - Local Authorities
     - Federal Authorities
     - Not Sure – Call PTAC
       - http://ptac.ed.gov/
  4. Develop a Communications Plan

DATA POLICIES TO PROTECT

DATA POLICIES

- Often informal policies or generally accepted in the district
- Often are not documented
- Recommendation
  - Make Policy OR
  - Make Admin Guideline OR
  - Make Internal Departmental Procedures
- Should be Periodically Reviewed

DATA PORTIONS OF CONTRACTS

- Included in contracts
- Standard Things to look for
  - FERPA, COPPA, etc references
  - Notification Standard for "Belief" of breach
  - Data Exchange Standards
    - Do NOT exchange data via email, whenever possible
    - SFTP (Secure File Transfer Protocol) Site
- Review language looking for data handling standards
- Have a Technology savvy solicitor review data & security areas of contract

DATA ACCESS AND USE POLICY

- Every user of every information system should sign a Data Access and Use Policy. The policy should inform the user of the following items:
  - As a user of an application, the information is considered confidential and the misuse can revoke a user's account at any time.
  - Any information contained in the database is considered district property and able to be subpoenaed in a court of law.
  - If a user believes that their login credentials have been compromised, they are to notify a district administrator immediately.
  - If a user believes to a breach has occurred to the system or contents of the system, they are to notify a district administrator immediately.
- Pennsylvania Department of Education (PDE) developed a Student Data Access and Use Policy that every superintendent should sign and fax to PDE.

DATA RELEASE POLICY

- A data release policy is critical to address internal and external data requests. In addition, establishing a request process or procedure with approvals of data stewards will help manage data releases.
- A data release policy should contain information on the following areas and note what approvals need to be obtained, if the release is approved.
- Ensure recipient understand confidentiality of data, perhaps signing a data confidentiality agreement.

Release Type	Requestor Type	Approving Authority
Student Assessment Information	External Use	Superintendent / School Board
Student Directory Information	Internal Staff	Data Council
Student Directory Information	Military	Data Council
Student Directory Information	Community	Superintendent / School Board
Student Discipline Information	Internal Staff	Data Council
Student Discipline Information	External Use	Data Council / Superintendent / School Board
Student Medical Information	Internal Staff	Data Council
Student Medical Information	External / School Community	Data Council / Superintendent / School Board

DATA DESTRUCTION POLICY

- The intent of this policy is to adhere to the FCC guidelines, FERPA, IDEA and other federal and state laws in regards to retaining and destroying data on a defined schedule.
- The policy must be aligned with state and federal retention mandates.
- Imperative that the Database Manager or Technology Director establish the appropriate destruction mechanisms or manual schedules to destroy the appropriate data.
- This will protect the district against allegations of selective document or record destruction.

VENDOR CONFIDENTIALITY AGREEMENT

- Vendors or consultants often assist school districts in implementing various products that contain staff, student or district information.
- Especially during a conversion process, the vendor will have at least one or multiple copies of the district's data at their location(s).
- A Vendor Confidentiality Agreement assures that the data possessed is not used for sales demonstrations, is destroyed after conversion is complete, ensures that users who interact with data have the appropriate clearances and it specifies a timeframe for a company to inform the district of a data breach.
- Each vendor that interacts with the Technology department should sign off on a confidentiality agreement and kept on record either with the Business Manager or Technology Director OR ensure that similar wording is included within the contract established with the vendor.
- This signed agreement often requested during a technology audit.

VENDOR DATA RELEASE AGREEMENT

- Many districts review the purchasing contract and look for problems or costs during the implementation phase. However, the agreement about data released back to the district upon termination of the contract is often overlooked.
- Three key areas should be addressed in the Vendor Data Release:
  1. All district data should be backed up and sent to the district in an agreed upon electronic format. Note that the database administrator should test the backups to make sure they contain data in a recoverable format.
  2. District data should be surrendered within ___ business days of written request from the district and within _____ business days of termination of contract.
  3. District data should be destroyed at the vendor's location within _____ business days of termination of contract. (Make sure to evaluate any state or federal laws around the application area before completing for vendor.)
- Each vendor that works with the Technology department should sign a Vendor Release Agreement OR ensure that similar wording is included within the contract established with the vendor.

QUESTIONS?

PRESENTED BY COLLEEN YENSER, PRSBO