Dayton Independent Schools

PII Data Security - Board Review

August 28, 2024 at 6:00pm

Current Measures to Prevent a Breach

- Anti-Virus/Malware/Spam/Spyware Protection
- Removing administrative role from user accounts on devices
  - This limits the ability to for malware or viruses to attack a device
- Office 365 Security Features/Policies Enabled
  - Multi-Factor Authentication Enabled
    - Text or Authentication APP
  - Prevent access to resources outside of the USA
    - Block Policy on All Office 365 accounts; including Student Accounts
- Vulnerability Scanning
    - CISA weekly scanning reports
- System Patch Management
  - Updates to Windows and Office products
  - Updates to Chrome OS (Chromebooks)
  - Updates to MacOS (Macbook and iMac devices)
  - Updates to IOS (iPADS)
- Cloud/Offsite Resources
- Active Directory/Group Policy Objects
- Private IP implementation
  - State maintained
- Distributed Denial of Service (DDOS) Mitigation
  - State maintained
- Web Filtration
  - New GoGuardian solution helps prevent access to malicious sites
- Centrally Managed Firewalls
  - State maintained
- Virtual Private Network Support
  - State maintains this service but provides districts access
- Secure File Transfer
  - Using encryption to securely transfer records
- Statewide Product Standards
  - This includes implementing a new Identity Management solution
    - This will be coming this school year
    - Managed student and staff identities – enabling and disabling automatically based on 1) employment of staff OR 2) enrollment of Student OR 3) non-paid staff contract
- Locked Data Center
- Locked File Cabinets/Doors
  - Securing Student records behind secure doors with limited physical access.
- Limited Access (Need to Know)
- Removal of user accounts for staff no longer employed (this will soon be automated)
- Staff confidentiality training and planned security training

- Continual communications to Staff regarding latest vulnerabilities in free or paid services.
- Continual email communications to Staff with examples of Phishing/SPAM emails to help prevent the accidental submission of PII data or systems account data to an attacker.

Informational Items

Current & Relevant Legislation

- **Federal**
  - FERPA (1974) – Family Rights and Privacy Act
  - COPPA (1998) – Children's Online Privacy Protection Act
  - CIPA (2000) – Children's Internet Protection Act
  - Others – IDEA, PPRA, etc.
- **State**
  - Kentucky FERPA (1994 – KRS 160.700 et seq.)
  - HB 232 (signed into law April 10, 2014)
  - HB 5 (signed into law April 10, 2014; effective January 1, 2015)
  - 702 KAR 1:170 (filed with LRC August 13, 2015)
  - CUES Project (Connected User Experience)
    - Vendor selected – RapidIdentity (Identity Management partner)
    - Automated system to create and disable systems accounts for Staff and Students
    - System connects into data systems such as Munis and Infinite Campus
    - Process to help keep systems secure by removing orphaned accounts that could cause data breaches

Relevant Board Policies & Procedures

- 01.61 – Records Management
- 01.61 AP.11 – Notice of Security Breach
- 09.14 – Student Records

House Bill 232

- Called for the creation of KRS 365.734
- Prohibits the certain uses of student data by cloud vendors
- Defines "student data"
- Requires cloud providers to certify in writing that they comply with the KRS

House Bill 5

- Called for the creation of KRS 61.931, 61.932, and 61.933
- Defines "Personal Information" (different from FERPA's definition of personally identifiable information or PII)
- Requires school districts to establish "reasonable security and breach investigation procedures and practices"
- Outlines security breach notification procedures and timelines

702 KAR 1:170

- Authorized by House Bills 5 and 232

- Requires that the district acknowledge to its local board prior to August 31 of each year that it has reviewed the guidance of the KAR and implemented best practices

Data Security and Breach Notification Best Practice Guide

Data Security and Breach Notification Best Practice Guide

Kentucky Department of Education (KDE)

V2.2 September 2015

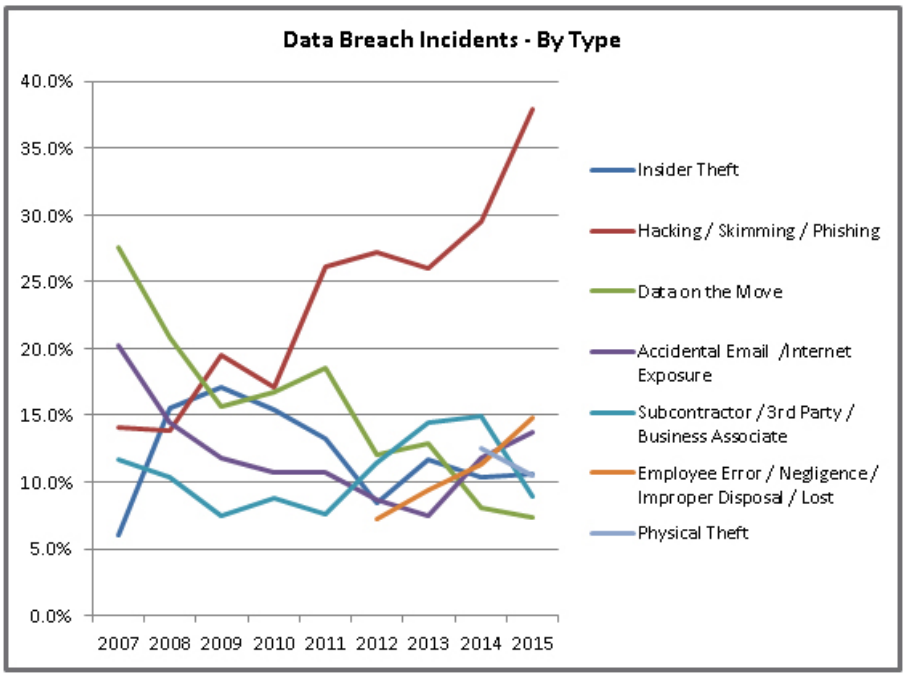
- Legislation requires KDE to create and update this guide
- Available for download here

Data Security Implementation Plan

- Identify and document data (both electronic and hard copy) that need to be protected
- Audit current access to data by various groups of people and make adjustments as needed
- Document data security measures and security breach procedures
- Provide awareness training with all staff who have access to confidential data

Main Causes of Data Breaches

• Human Error
  • Accidental sharing (email, website, paper, etc.)
  • Weak or stolen passwords
  • Loss or theft of employee device (USB drive, laptop…)
  • Phishing, clickbait
	• Everything Else
	  • Application vulnerabilities – unpatched software
	  • Hackers
	  • Malware



Source: Identity Theft Resource Center: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

Confidential Data

- Student education records except "directory" information in certain circumstances
- PII as defined by FERPA and House Bill 5

Security Breach Notification

Notify all individuals and agencies as outlined in KRS 61.933 if PII has been disclosed and will result in the likelihood of harm to one or more persons

One of these		One or more of these
• First name or first initial and last name • Personal mark • Unique biometric print/image	**AND**	• Account number with PIN that would allow access to the account • Social Security Number • Taxpayer ID number • Driver's license number or other ID number issued by any agency (student ID number) • Passport number or other number issued by the US • Individually identifiable health information except for education records covered by FERPA

Student Data

- "Student data" means any information or material, in any medium or format, that concerns a student and is created or provided by the student in the course of the student's use of cloud computing services, or by an agent or employee of the educational institution in connection with the cloud computing services. Student data includes the student's name, email address, email messages, postal address, phone number, and any documents, photos, or unique identifiers relating to the student. (KRS 365.734)

Cloud Providers

- KRS 365.734 prohibits cloud providers from processing student data for any purpose other that improving its services. Specifically prohibits use of data for advertising and selling of student data.
- Current cloud providers/programs: Infinite Campus, Pearson (CIITS and others), NWEA (MAP), Microsoft, Lexia, AIMS Web, WIDA, Career Cruising, KET Encyclomedia, Reading Plus, Remind, Khan Academy, KidBlog, Prezi, and More …