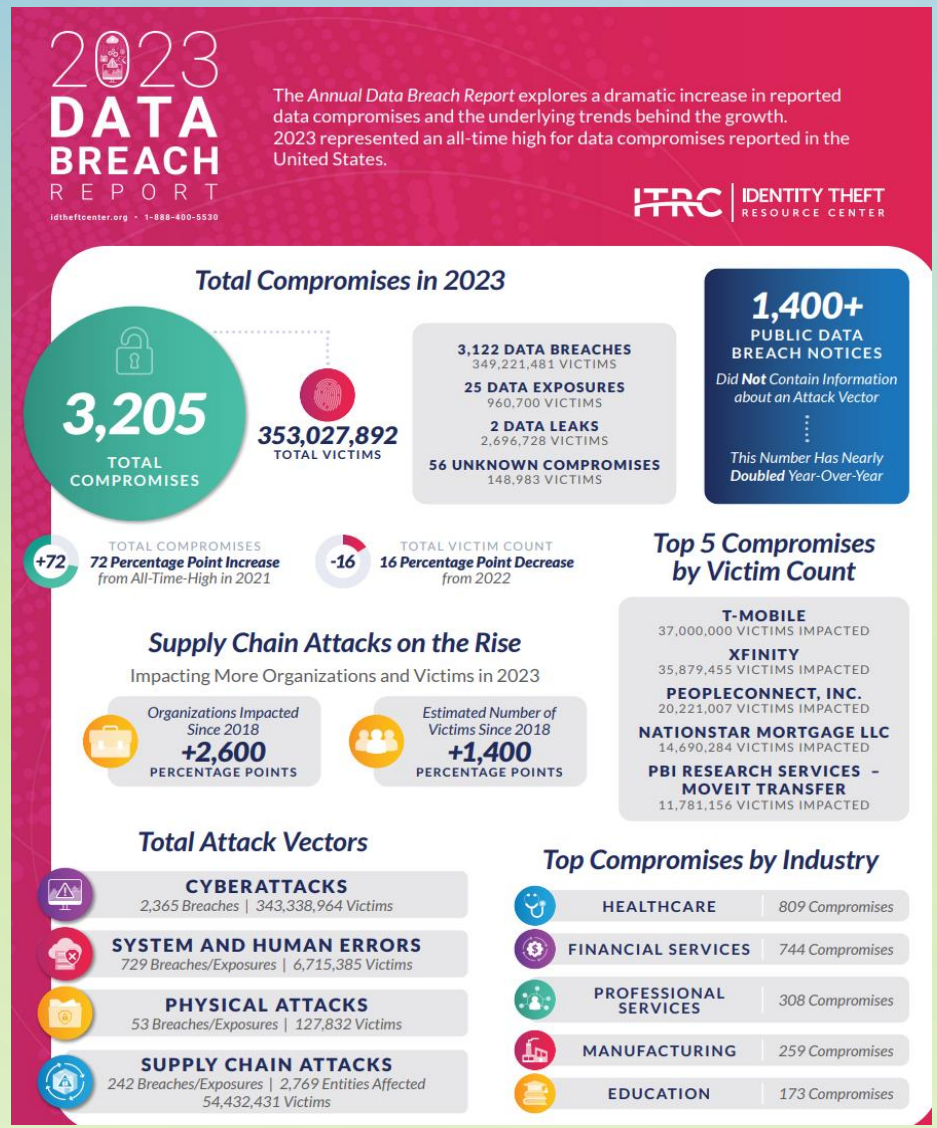
Data and Security

Marion County Board of Education

Purpose

- Basic awareness of data security and privacy best practices
- Notification to the local board that the district has reviewed and implemented best practices

DATA BREACH REPORT



via
Identity Theft Resource Center
https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf

EXAMPLES OF SECURITY BREACH

Highline Public Schools, a 17,500-student district south of Seattle, canceled classes for Sep. 9 due to a cyberattack. In an announcement posted Sep. 8, the district said it had “detected unauthorized activity on our technology systems and have taken immediate action to isolate critical systems. We are working closely with third-party, state and federal partners to safely restore and test our systems.” The closure impacts all school activities, athletics and meetings for the district. The Seattle Times reports that the loss of computer access due to the attack disables communications systems, the ability to dispatch buses and other transportation, and updates to attendance records, according to a district spokesperson

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.) – non release student data
- HB 232 (signed into law April 10, 2014) – cloud providers cannot share PII
- HB 5 (signed into law April 10, 2014; effective January 1, 2015) – breach of security investigation
- 702 KAR 1:170 (filed with LRC August 13, 2015) – share policies with local board

KRS 365.734

- Requires cloud providers to certify in writing that they comply with the KRS
- Prohibits the certain uses of student data by cloud vendors
- Defines “student data”

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.
  - 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.
- Current cloud providers/programs: Infinite Campus, Pearson, iReady Google, Microsoft, Edmentum, Follett, Clever

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

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

MARION COUNTY SCHOOLS SECURITY REPORT CARD

CYBER HYGIENE

REPORT CARD

Marion County Schools

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

CYBER+INFRASTRUCTURE

HIGH LEVEL FINDINGS

LATEST SCANS

May 31, 2024 — August 1, 2024
Completed host scan on all assets

July 30, 2024 — August 1, 2024
Last vulnerability scan on all hosts

ASSETS OWNED
154
No Change

ASSETS SCANNED
154
No Change
100% of assets scanned

HOSTS
2
No Change

SERVICES
4
No Change

VULNERABLE HOSTS
0
No Change
0% of hosts vulnerable

VULNERABILITIES
0
No Change

VULNERABILITIES

SEVERITY BY PROMINENCE

0 CRITICAL 0 RESOLVED 0 NEW
0 HIGH 0 RESOLVED 0 NEW
0 MEDIUM 0 RESOLVED 0 NEW
0 LOW 0 RESOLVED 0 NEW

VULNERABILITY RESPONSE TIME

0 DAYS
0 Days — 15+ Days
MAX AGE OF ACTIVE CRITICALS

0 DAYS
0 Days — 30+ Days
MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0	FTP 0
Telnet* 0	RPC 0
SMB* 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open · Open, No New · Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

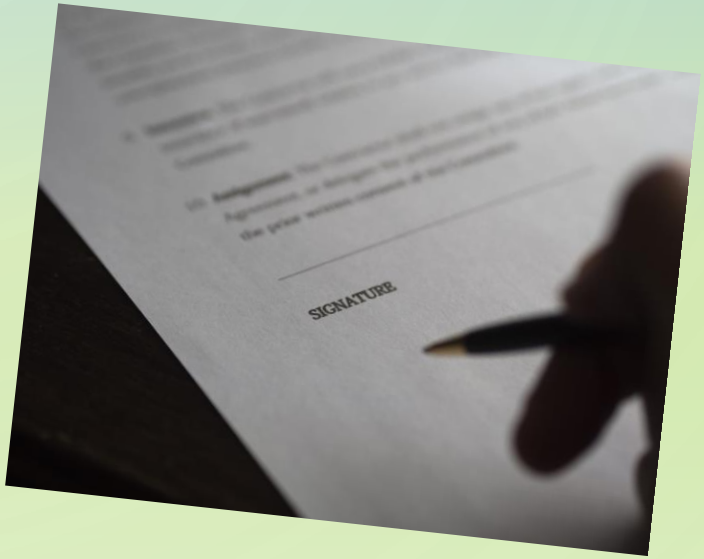
** Denotes the possibility of a network management interface.*

Current Measures to Prevent a Breach

- Anti-Virus/Malware/Spam/Spyware Protection
- Vulnerability Scanning
- System Patch Management
- Cloud/Offsite Resources
- Active Directory/Group Policy Objects
- Private IP implementation
- Distributed Denial of Service (DDOS) Mitigation
- Web Filtration
- Centrally Managed Firewalls
- Virtual Private Network Support
- Secure File Transfer
- Statewide Product Standards
- Locked Data Center
- Locked File Cabinets/Doors
- Limited Access
- Disable/removal of user accounts for staff no longer employed
- Staff confidentiality training and planned security training

DATA SHARING AGREEMENT

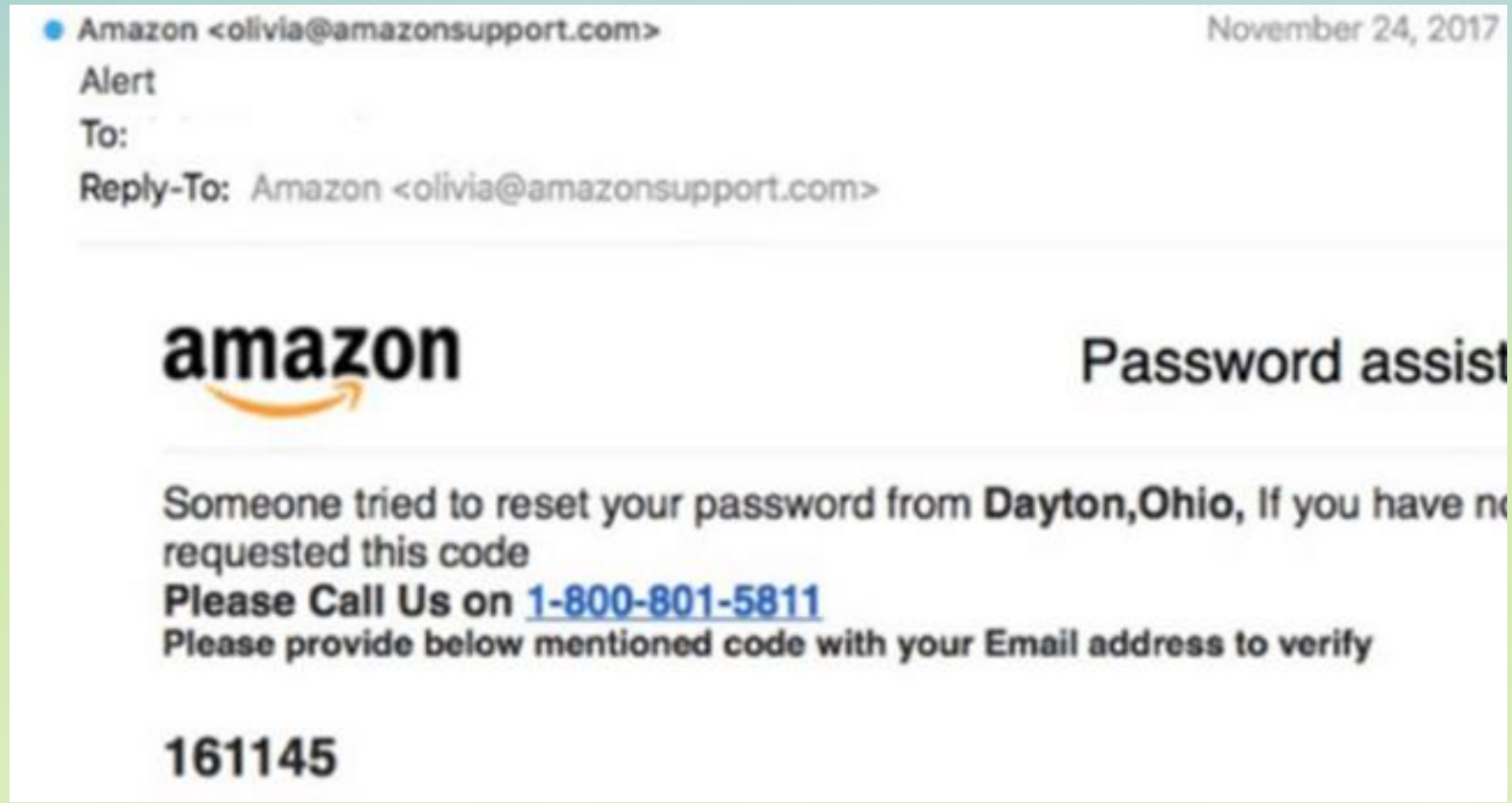
- A data sharing agreement MUST exist between the district and the third party when student data is involved.
- Rule of thumb: get a data sharing agreement anytime students will have individual accounts.



COMMON CAUSES OF SECURITY BREACH

- Access Control Breaches
- Malware Attacks
- Phishing and Social Engineering
- Denial of Service Attack
- Insider Threats
- Supply Chain Attacks
- Physical Security Breaches

PHISHING EXAMPLE



Amazon <olivia@amazonsupport.com> November 24, 2017

Alert

To:

Reply-To: Amazon <olivia@amazonsupport.com>

amazon Password assist

Someone tried to reset your password from **Dayton,Ohio,** If you have n
requested this code

Please Call Us on 1-800-801-5811

Please provide below mentioned code with your Email address to verify

161145

PASSWORDS

- Use complex passwords
- Change them regularly – like toothbrushes
- DO NOT use passwords based on “password” or the names of the seasons, months, family members, pets, or sports teams. Everyone uses them so they are VERY predictable and the first ones a hacker will try
- Use long AND memorable passwords or passPHRASES like “4sCORE&5evnYrs” (four score and seven
- years) which is easy to remember, but cannot be easily guessed

DON'T GIVE OUT

Your (or your family members'):

- **First or last name**
- **Date of birth**
- **Social security number**
- **Address, school, employer, etc.**
- **Relationship to anyone mentioned in the conversation**
- **Credit card or bank account numbers**