


Data and Security

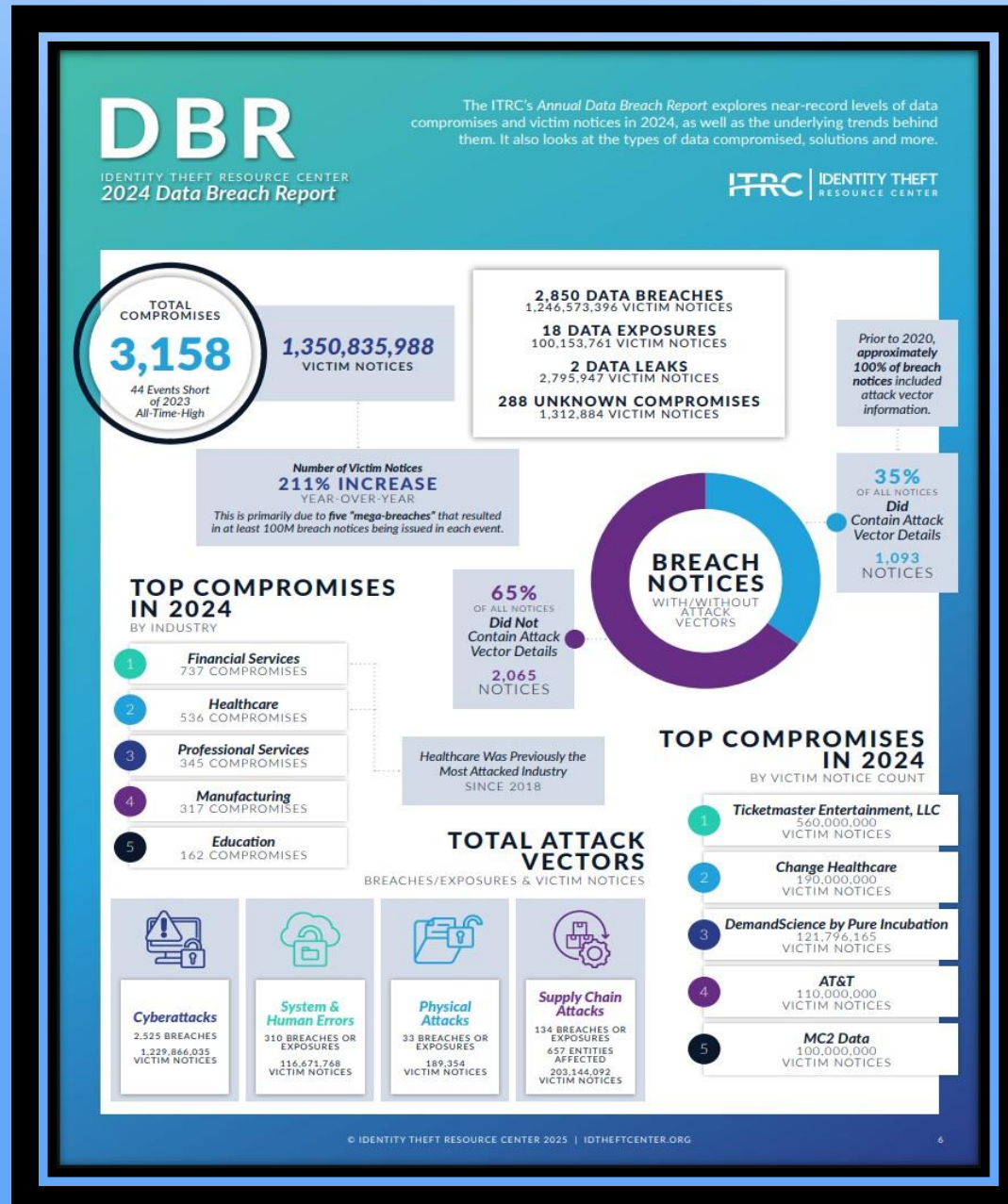
Marion County Board of Education



Purpose

- Basic awareness of data security and privacy best practices
 - Notification to the local board that the district has reviewed and implemented best practices
- 
- A series of three parallel white diagonal lines in the bottom right corner of the slide, extending from the middle of the right edge towards the bottom left.

DATA BREACH REPORT FOR UNITED STATES



- Total number of compromises remained flat compared to 2024
- Five mega breaches (100M breaches/event) increased the victim notices by 211%
- Exclude the mega breaches – victim notices (accounts compromised) decreased by 47%
- Financial Services most breached, followed by healthcare services
- Cyberattacks – root cause of data breaches

Identity Theft Resource Center
https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf

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



This Photo by Unknown Author is licensed under
CC BY-NC-ND

Current & Relevant Legislation

Federal

- FERPA (1974) – Family Rights and Privacy Act
 - Schools are required to protect personally identifiable information (name, address, ss#, etc)
- COPPA (1998) – Children’s Online Privacy Protection Act
 - Requires websites/online services for children under 13 years of age
- CIPA (2000) – Children’s Internet Protection Act (Internet Safety for Schools & Libraries)
 - Requires E-rate districts to put in place technology protection measures
- Others – IDEA, PPRA, etc.

State

- Kentucky FERPA (1994 – KRS 160.700 et seq.) – non-release of 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) – districts required to investigate security breaches
- 702 KAR 1:170 (filed with LRC August 13, 2015) – requires districts to annually review data security guide



This Photo by Unknown Author is licensed under
CC BY-NC-ND

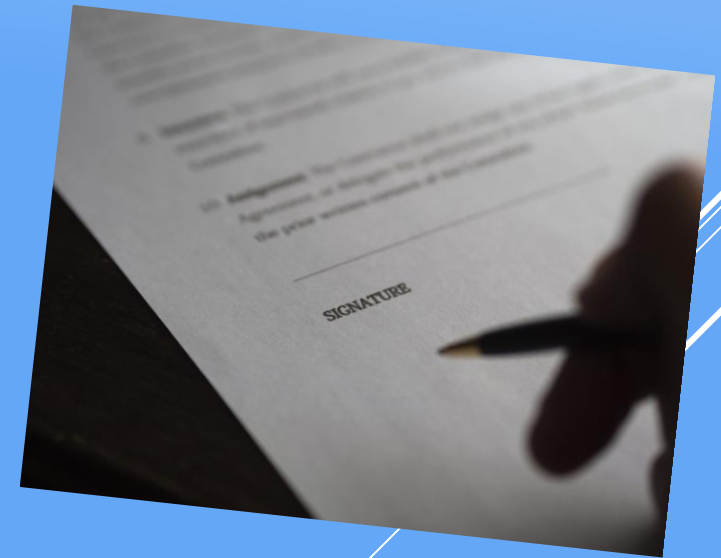
CLOUD PROVIDERS

- KRS 365.734 prohibits cloud providers from processing student data for any purpose other than improving their services.
- Student Data Includes: Name, email, messages, photos, unique identifiers
- Current cloud providers/programs: Infinite Campus, Pearson, iReady Google, Microsoft, Edmentum, Follett, Clever



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.



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
<ul style="list-style-type: none">• First name or first initial and last name• Personal mark• Unique biometric print/image	AND	<ul style="list-style-type: none">• 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

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



CYBER HYGIENE

REPORT CARD

Marion County Schools



0
Hosts with
unsupported
software



0
Potentially Risky
Open Services



0%
No Change in
Vulnerable
Hosts

**CISA**
CYBER+INFRASTRUCTURE

HIGH LEVEL FINDINGS

LATEST SCANS

May 27, 2025 — June 28, 2025

Completed host scan on all assets

June 25, 2025 — June 28, 2025

Last vulnerability scan on all hosts

ASSETS OWNED

154

No Change

HOSTS

2

No Change

VULNERABLE HOSTS

0

No Change
0% of hosts vulnerable

ASSETS SCANNED

154

No Change
100% of assets scanned

SERVICES

4

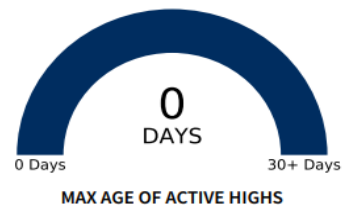
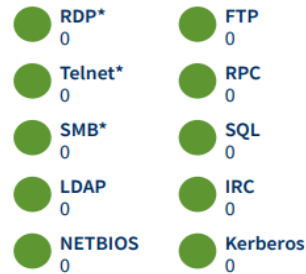
No Change

VULNERABILITIES

0

No Change

VULNERABILITIES

SEVERITY BY
PROMINENCEVULNERABILITY
RESPONSE TIMEPOTENTIALLY RISKY
OPEN SERVICES

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.

MARION COUNTY SCHOOLS SECURITY REPORT CARD

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
- DMARC Compliant Email Domain
- MFA
- 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
- 15 character password for staff