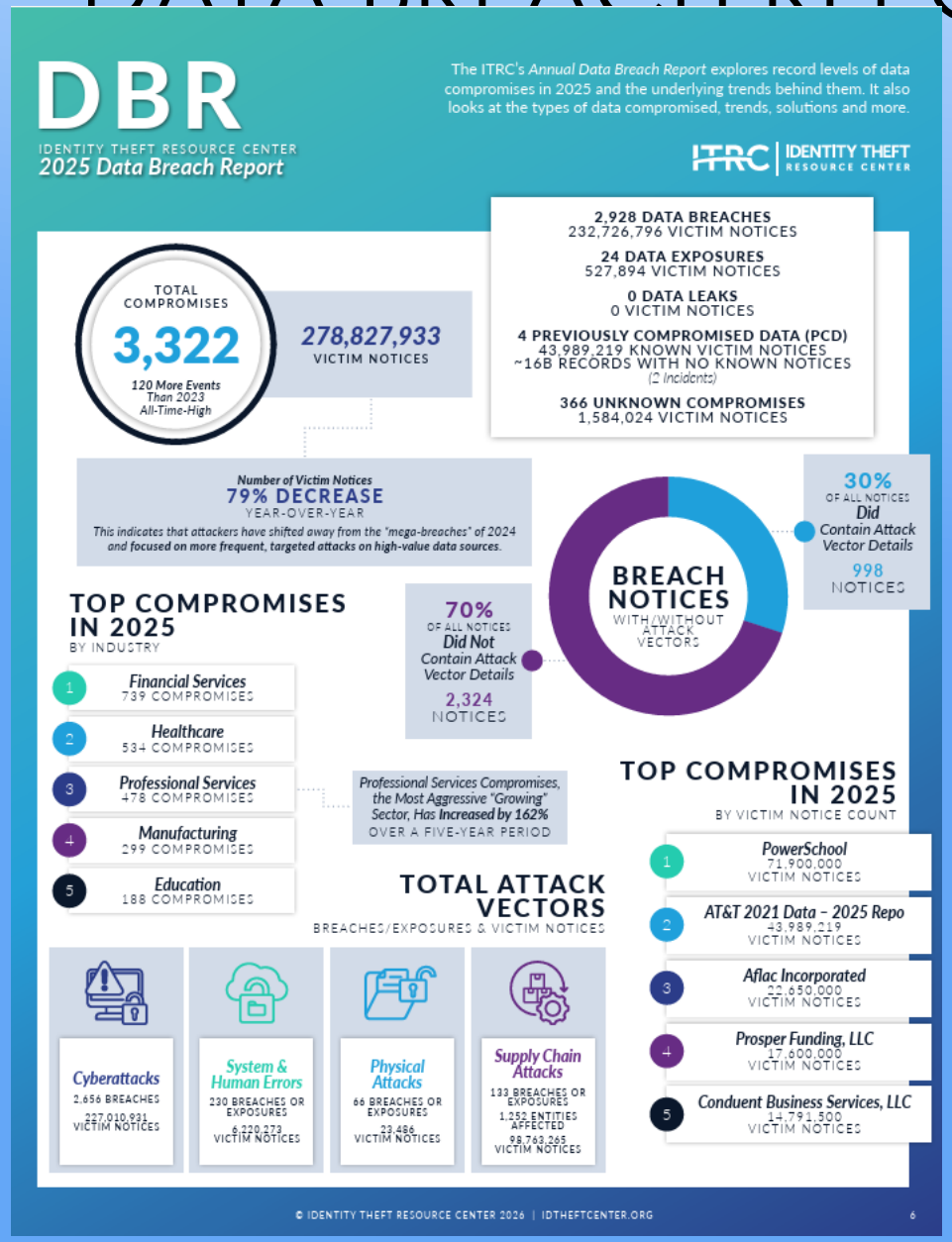
Data and Security

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 FOR UNITED STATES



- **3,322 total compromises** (data breaches, exposures, leaks, and unknown incidents) were reported in 2025, a **20% increase** over the previous record set in 2023.
- Victim notices **decreased by 79% year over year**, suggesting attackers shifted away from massive "mega-breaches" toward **more frequent, targeted attacks** on high-value data sources.

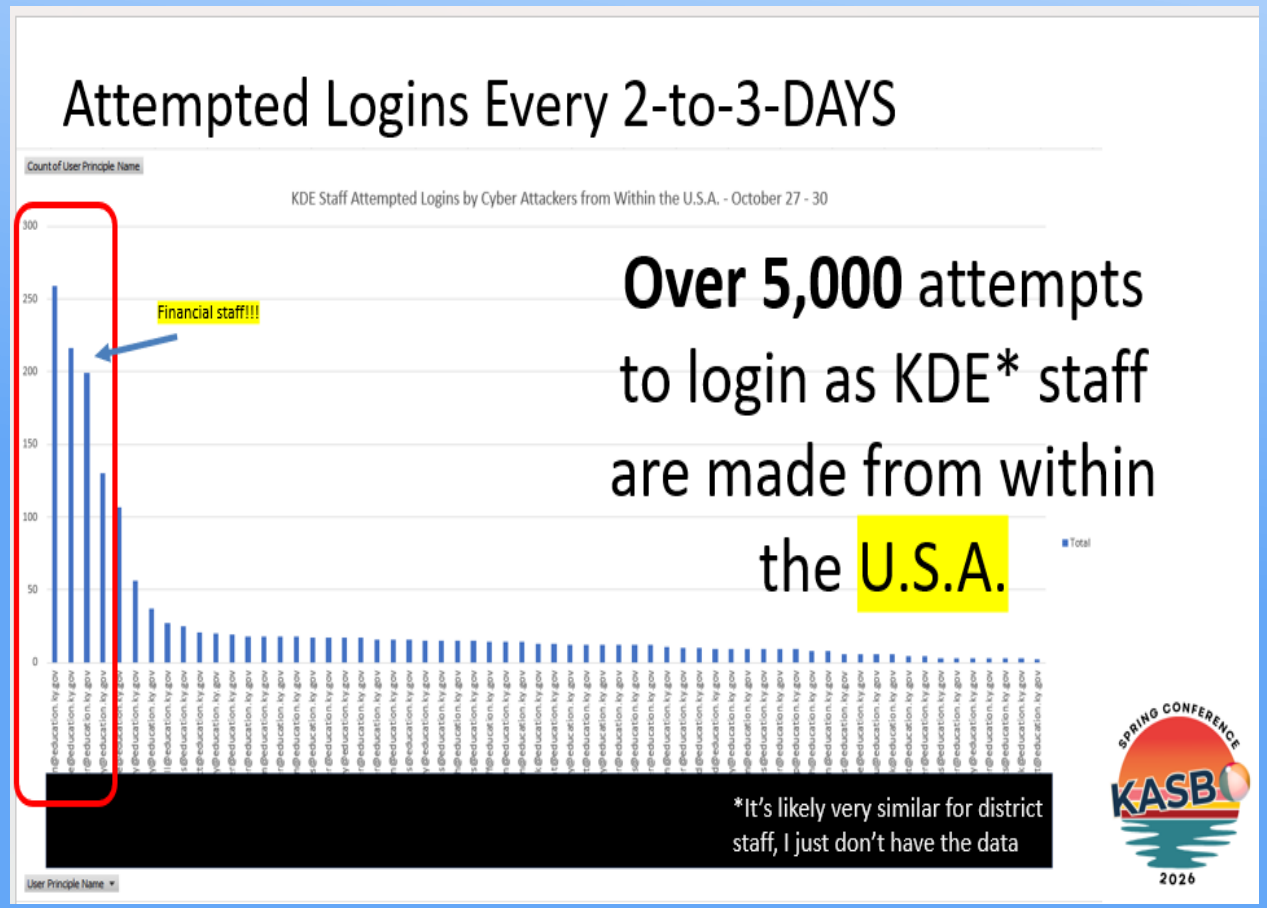
Industries with the Most Compromises

Financial Services – 739 compromises.
Healthcare – 534.
Professional Services – 478 (grew 162% over five years).
Manufacturing – 298.
Education – 188.

Identity Theft Resource Center
https://www.idtheftcenter.org/publication/2025-data-breach-report/

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



KDE STAFF ATTEMPTED LOGINS BY CYBER ATTACKERS

- This slide highlights the frequency of attempted unauthorized logins targeting KDE staff accounts.
- Attempted login attacks occur every 2–3 days.
- More than 5,000 login attempts were made to access KDE staff accounts from within the United States during the reporting period (October 27–30).
- Financial staff most attempted logins

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

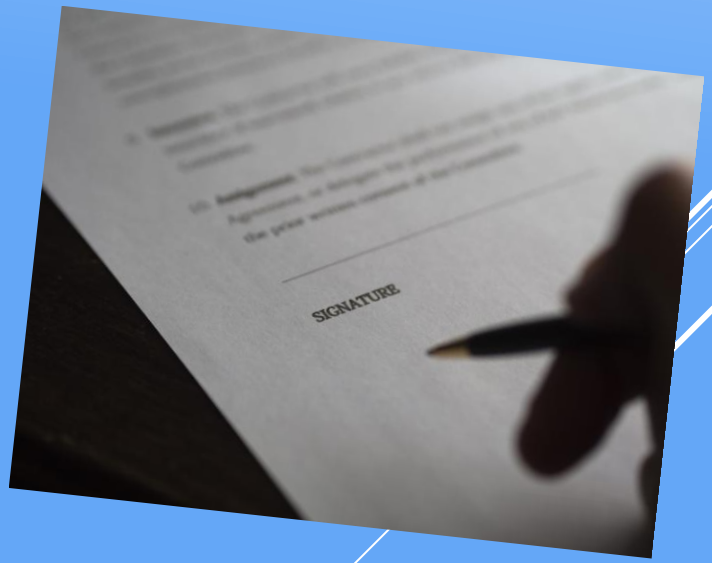
- Kentucky FERPA (1994 – KRS 160.700 et seq.) – non-release of student data
- HB 232 (signed into law April 10, 2014) – cloud providers cannot share PII
- HB 5 (signed into law April 10, 2014; effective January 1, 2015) – districts required to investigate security breaches
- 702 KAR 1:170 (filed with LRC August 13, 2015) – requires districts to annually review data security guide

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
• 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

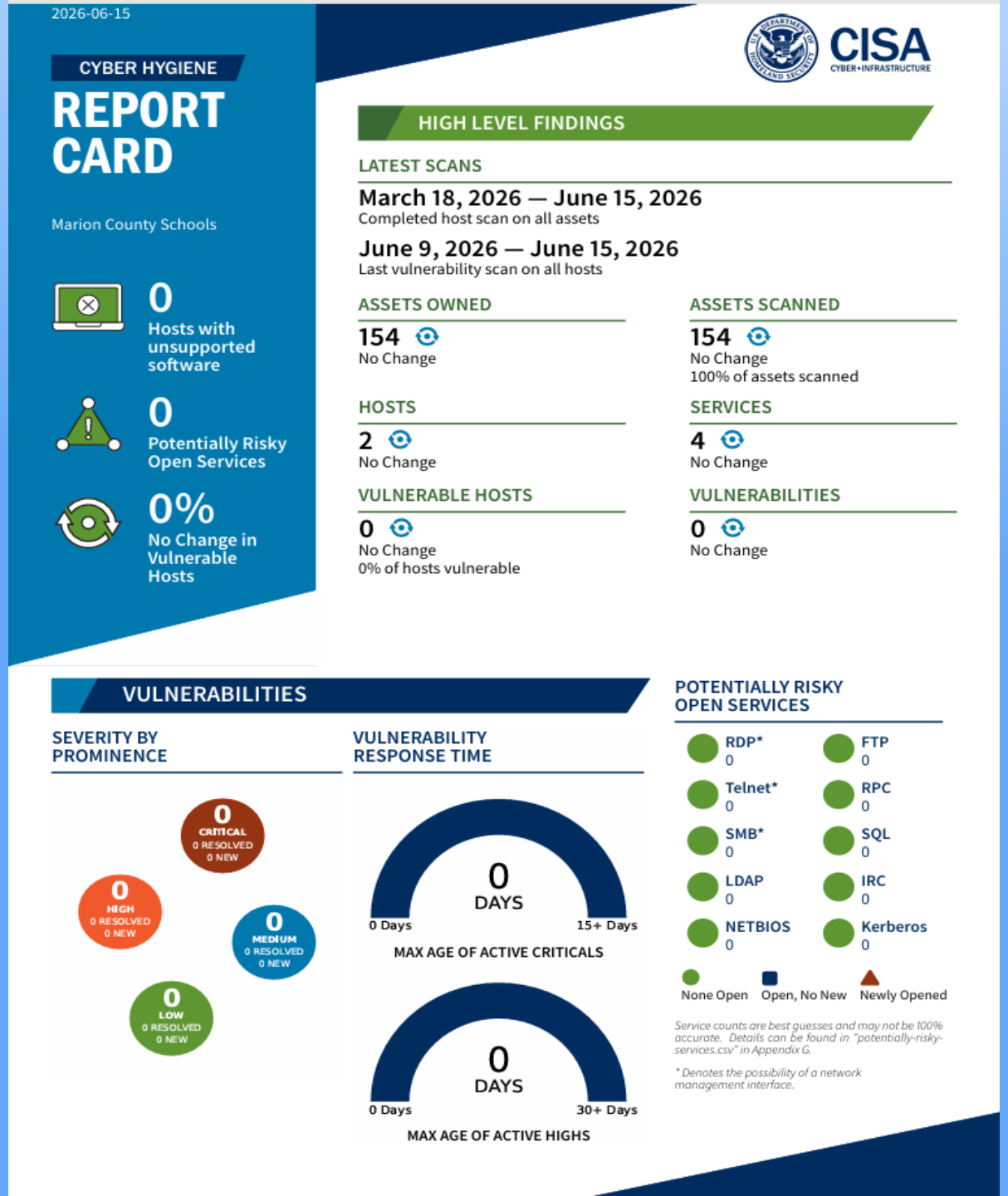
Main Causes of Data Breaches

Human Error

- Accidental sharing (email, website, paper, etc.)
- Weak or stolen passwords
- Loss or theft of employee device (USB drive, laptop…)
- Phishing, social engineering

Other Sources

- Application vulnerabilities – unpatched software
- Hackers
- Third Party Vendors



MARION COUNTY SCHOOLS SECURITY REPORT CARD

- Maintained a strong cybersecurity posture
- 100% of known assets were successfully scanned.
- No known vulnerabilities were detected across scanned systems.
- No unsupported software was identified.
- No risky internet-facing services were exposed.
- No vulnerable hosts were found.

Current Measures to Prevent a Breach

- Anti-Virus/Malware/Spam/Spyware Protection
- PhishId – vulnerability scan
- 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 - email protocol, to protect email domain (New)
- MFA – for all staff and students (NEW)
- 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