# *Special Report*

***Arkansas Legislative Audit***

# Cybersecurity Incidents Reported by Public Entities

For the Period July 1, 2024 through June 30, 2025




## INTRODUCTION

This report is issued pursuant to Ark. Code Ann. § 10-4-429, which requires Arkansas Legislative Audit (ALA) to compile, and submit to the General Assembly, an annual list of all cybersecurity incidents reported to ALA by a public entity. For the purposes of this report, the term "public entity" refers generically to organizations at all levels of Arkansas government, including state agencies, counties, municipalities, school districts, higher education institutions, etc. A "cybersecurity incident" is any event that compromises the security, confidentiality, or integrity of an entity's information systems, applications, data, or networks.

## OBJECTIVE

The objective of this report is to provide the General Assembly with the annual compilation of cybersecurity incidents reported to ALA under Ark. Code Ann. § 10-4-429, which is provided in **Appendix A**.

## SCOPE AND METHODOLOGY

The cybersecurity incidents included in this report were reported to ALA by public entities during the period July 1, 2024 through June 30, 2025. This report discloses the type of incidents reported and the response process from the time the incident was detected through remediation steps taken. It does not include the various continuous processes and controls public entities have in place to monitor and identify potential cybersecurity incidents. The types of cybersecurity incidents reported are defined in **Appendix B**.

## BACKGROUND

Public entities invest a substantial amount of resources in their information assets, including computers, networks, programs, and data; hardware equipment and software; internet access; and personnel training. Furthermore, public entities rely on this technology to store, process, and report financial and non-financial information and conduct business with citizens, as well as other local, state, and federal agencies. This reliance on technology, combined with the growing sophistication of individuals or groups with malicious intent, places public entities at increasing risk for a cybersecurity incident, which can negatively affect an entity's financial health and reputation and citizens' ability to conduct business with them.

Prior to the passage of Act 260 of the 2021 Regular Session (codified at Ark. Code Ann. § 10-4-429), there was no requirement for public entities in Arkansas to report cybersecurity incidents. ALA often detected such incidents during routine audit procedures or learned of them through media reports. The General Assembly recognized that a mechanism should be in place to collect information pertaining to cybersecurity incidents occurring at public entities throughout the State and evaluate these incidents so that proactive measures can be taken to prevent disruption of government operations.

**ARKANSAS LEGISLATIVE AUDIT**
500 Woodlane Street, Suite 172, Little Rock, AR 72201
Phone: 501-683-8600 • Fax: 501-683-8605
www.arklegaudit.gov

Report ID: SPIS00425 Report Date: June 30, 2025

### Legislative Update

During the Regular Session of 2025, the Arkansas General Assembly enacted the Arkansas Cybersecurity Act of 2025 (Act 489), which centralizes the approach to defending state government systems against cyber threats. This legislation addresses the growing frequency and sophistication of cyberattacks, which pose risks to state data and infrastructure, as well as public trust.

Act 489 created the State Cybersecurity Office (Office), which is part of the Department of Shared Administrative Services and is led by the State Information Security Officer (Officer). This Office is responsible for providing centralized oversight and coordination of cybersecurity efforts across all state agencies. The Officer's duties include setting statewide security standards, managing incident response, conducting audits of state agency compliance with cybersecurity governance standards, coordinating threat detection, and ensuring that mandatory cybersecurity training is provided.

Under Act 489, state agencies are required to report on cybersecurity matters to the Office while retaining control over their day-to-day operations. This centralization of oversight, combined with agencies' expertise over their internal information technology (IT) environments, enhances Arkansas's ability to safeguard its digital infrastructure and address cyber threats and represents a significant advancement in the State's cybersecurity governance. Additionally, the Office is required to submit reports to the legislature at least twice a year, detailing assessments, progress on remediation, and any instances of noncompliance.

The overarching goal of Act 489 is to create a more resilient and secure digital infrastructure for Arkansas, safeguarding both government operations and sensitive citizen data. The push for centralization reflects a broader trend of recognizing cybersecurity as a critical statewide function rather than a fragmented effort among individual agencies.

## RESULTS OF REVIEW

### Summary of Cybersecurity Incidents Reported

During the period July 1, 2024 through June 30, 2025, a total of 217 cybersecurity incidents were reported to ALA by 124 public entities at all levels of state government. A complete list of these incidents is provided in **Appendix C**. Of the 217 incidents reported, 193 have been resolved, and 24 remain under investigation. A list by entity type and incident type is provided in **Appendix D**. Additionally, **Exhibit I** provides a summary of incidents by type for fiscal years 2022, 2023, 2024, and 2025. **Exhibit II on page 3** charts the incidents reported in fiscal year 2025 based on the month in which they were reported to ALA, and **Exhibit III on page 3** charts the incidents based on the month in which they occurred. As shown in **Exhibit IV on page 4**, the number of reports increased by 64% from fiscal year 2024 to fiscal year 2025.

**Exhibit I**

**Cybersecurity Incidents Reported to Arkansas Legislative Audit by Incident Type For Fiscal Years 2022 through 2025**

| | Number of Incidents Reported By Fiscal Year | | | |
|---|---|---|---|---|
| Incident Type | 2022* | 2023 | 2024 | 2025 |
| Breach of Confidentially | 8 | 7 | 10 | 8 |
| Brute Force Attack | 1 | 0 | 1 | 1 |
| Business Email Compromise | 1 | 0 | 9 | 22 |
| Cross-Site Scripting | 0 | 0 | 0 | 1 |
| Fraudulent Transaction | 23 | 52 | 29 | 48 |
| Loss or Theft of Equipment | 3 | 0 | 1 | 1 |
| Malware Attack | 2 | 3 | 8 | 6 |
| Ransomware | 4 | 16 | 6 | 9 |
| Spam or Phishing Attack | 1 | 26 | 41 | 60 |
| Unauthorized Access | 20 | 26 | 27 | 61 |
| **Total** | **63** | **130** | **132** | **217** |

*The reporting period began on July 28, 2021.

***Source**: Incident reports submitted by public entities (unaudited by Arkansas Legislative Audit)*

## Exhibit II

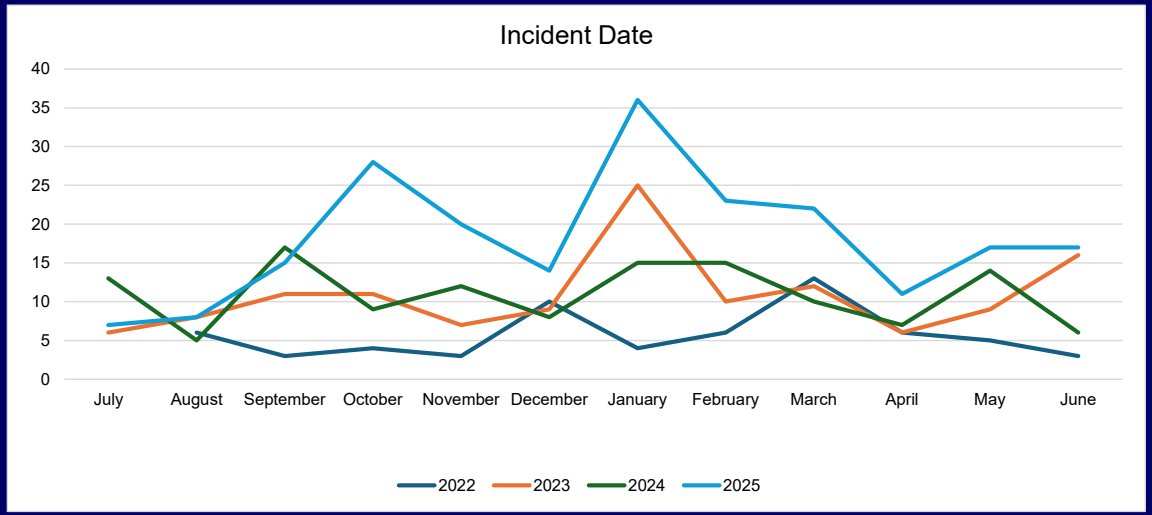
### Cybersecurity Incident Chart
### By Month Incident Was Reported to Arkansas Legislative Audit (ALA)
### For the Period July 1, 2024 through June 30, 2025

| | Month Reported to ALA | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2024 | | | | | | 2025 | | | | | | Incident Type Totals |
| Incident Type | Jul | Aug | Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | |
| Breach of Confidentially | 1 | 2 | | | 1 | 1 | | | 2 | | | 1 | **8** |
| Brute Force Attack | | | | | | 1 | | | | | | | **1** |
| Business Email Compromise | 2 | | 2 | 3 | 3 | 3 | 1 | | 2 | 3 | | 3 | **22** |
| Cross-Site Scripting | | | 1 | | | | | | | | | | **1** |
| Fraudulent Transaction | 2 | 5 | 4 | 3 | 2 | | 9 | 11 | 2 | 3 | 4 | 3 | **48** |
| Loss or Theft of Equipment | | | | 1 | | | | | | | | | **1** |
| Malware Attack | | | 1 | | | 2 | | | 1 | 1 | 1 | | **6** |
| Ransomware | | 1 | | | 1 | 1 | 1 | | 1 | | 2 | 2 | **9** |
| Spam or Phishing Attack | 2 | 2 | 2 | 8 | 5 | | 4 | 10 | 10 | 6 | 5 | 6 | **60** |
| Unauthorized Access | 1 | 3 | 8 | 6 | 11 | 8 | 3 | 4 | 4 | 4 | 2 | 7 | **61** |
| **Monthly Totals** | **8** | **13** | **18** | **21** | **23** | **16** | **18** | **25** | **22** | **17** | **14** | **22** | **217** |

***Source***: *Incident reports submitted by public entities (unaudited by Arkansas Legislative Audit)*

## Exhibit III

### Cybersecurity Incident Graph
### By Month Incident Occurred
### For the Period July 1, 2024 through June 30, 2025

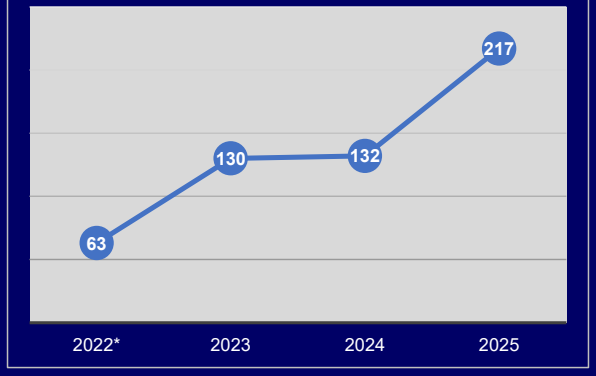



***Source***: *Incident reports submitted by public entities (unaudited by Arkansas Legislative Audit)*

Of the 217 incidents reported, 177 were reported to ALA within 5 business days of detection, in accordance with Ark. Code Ann. § 10-4-429, while 40 incidents (18.4%) were not reported timely. Some entities indicated they were not aware of the requirement to report until notified by their auditors, vendors, or other entities.

**Exhibit IV**

**Cybersecurity Incidents Reported to Arkansas Legislative Audit by Fiscal Year For Fiscal Years 2022 through 2025**




*The reporting period began on July 28, 2021.

***Source**: Incident reports submitted by public entities (unaudited by Arkansas Legislative Audit)*

### Significant Cybersecurity Incidents

During the review period, incident reports related to ransomware revealed the involvement of foreign threat actors. Several highly active ransomware and data extortion groups have been operating in Arkansas since at least July 2023. These groups target various industries across multiple continents, are known for their sophisticated tactics, and employ various families of malware to execute their attacks. These groups also collaborate with other hacker groups to encrypt and exfiltrate data from targeted organizations, subsequently demanding a ransom for return of the data. These foreign threat actors appear to be responsible for at least six incidents reported to ALA. Despite the rise in incidents, there were no reports of ransom payments made by public entities in Arkansas during fiscal year 2025.

The types of incidents that caused the most harm included business email compromise scams, spam or phishing attacks, and fraudulent transactions. Many of these incidents originated from email requests made by malicious actors impersonating legitimate vendors or employees, asking for changes to bank routing and account numbers. Although the frequency of these incidents has increased, the response from state and local governments to prevent and mitigate damages demonstrates an awareness of the ongoing threats and the necessary measures to address them.

## SUMMARY

Act 260 of the 2021 Regular Session (codified at Ark. Code Ann. § 10-4-429) was enacted to require public entities in Arkansas to report cybersecurity incidents to ALA and requires ALA to compile and submit annually a list of incidents to the General Assembly. The collection of information about these incidents could encourage implementation of measures to prevent disruption of government operations.

Cybersecurity threats facing Arkansas public entities are continuously evolving and increasing in number. As shown in **Exhibit I on page 2**, a total of 217 cybersecurity incidents were reported to ALA by 124 public entities. Of the 217 incidents reported, 193 have been resolved, and 24 remain under investigation, as shown in **Appendix C**.

During the Regular Session of 2025, the Arkansas General Assembly enacted Act 489, which created the State Cybersecurity Office as part of the Department of Shared Administrative Services. This Office is led by the State Information Security Officer.

Given the evolving nature of cybersecurity threats across government levels, it is imperative that the State continue its proactive approach to cybersecurity. Recognizing that cybersecurity incidents will inevitably occur, causing harm and operational disruptions, preparation becomes paramount to minimizing interruptions, protecting sensitive information, and maintaining public and employee confidence in the safety and security of government networks.

# APPENDICES

**Appendix A:** Ark. Code Ann. § 10-4-429

**Appendix B:** Glossary of Cybersecurity Incident Terms

**Appendix C:** Complete List of Cybersecurity Incidents Reported to Arkansas Legislative Audit by a Public Entity − For the Period July 1, 2024 through June 30, 2025

**Appendix D:** List of Cybersecurity Incidents Reported to Arkansas Legislative Audit − By Entity Type − For the Period July 1, 2024 through June 30, 2025

## Appendix A

## Ark. Code Ann. § 10-4-429

**(a)** As used in this section:

**(1)** "Public entity" means an entity of the state, political subdivision of the state, or school; and

**(2)** "Security incident" means any compromise of the security, confidentiality, or integrity of an information system maintained by a public entity, a contractual provider of an information system that contracts with a public entity, or other computer-related services of a public entity, that is caused by any unauthorized:

**(A)** Access to an information system of a public entity;

**(B)** Destruction of an information system of a public entity or the data of an information system of a public entity; or

**(C)** Acquisition of data from an information system of a public entity.

**(b)**

**(1)** A public entity that experiences a security incident shall disclose, in writing, an initial report of the known facts of the security incident to the Legislative Auditor within five (5) business days after learning of the security incident.

**(2)** A public entity shall provide regular updates of the security incident to the Legislative Auditor until the investigation of the security incident is closed.

**(c)** The Legislative Auditor shall:

**(1)** Maintain a list of all security incidents reported by a public entity; and

**(2)** Annually on or before December 15, report the information required by subdivision (c)(1) of this section to the Legislative Council, Legislative Joint Auditing Committee, and Joint Committee on Advanced Communications and Information Technology.

**(d)** If the Legislative Auditor believes the security incident significantly compromises citizens' data, creates a significant security concern, or involves significant theft, then the Legislative Auditor shall notify:

**(1)** The Governor;

**(2)** The President Pro Tempore of the Senate;

**(3)** The Speaker of the House of Representatives;

**(4)** The House and Senate cochairs of the Legislative Council;

**(5)** The cochairs and the co-vice chairs of the Legislative Joint Auditing Committee; and

**(6)** The cochairs of the Joint Committee on Advanced Communications and Information Technology.

**(e)** A report, update, notification, or list created or maintained under this section is exempt from disclosure under the Freedom of Information Act of 1967, § 25-19-101 et seq., as a security function under § 25-19-105(b)(11).

Amended by Act 2023, No. 175, § 2, eff. 8/1/2023.

## Appendix B

## Glossary of Cybersecurity Incident Terms

| Term | Definition | Source |
|---|---|---|
| **Breach of Confidentiality** | Unauthorized acquisition, access, use, or disclosure of confidential information that compromises the security, confidentiality, or integrity of the information. | 1 |
| **Brute Force Attack** | A method of accessing an obstructed device by attempting multiple combinations of numeric/alphanumeric passwords. | 2 |
| **Business Email Compromise** | A sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests. | 3 |
| **Cross-Site Scripting** | A security flaw found in some web applications that enables unauthorized parties to cause client-side scripts to be executed by other users of the web application. | 2 |
| **Fraudulent Transaction** | The unauthorized use of accounts or payment information; can result in the loss of funds, property, or information. | 4 |
| **Loss or Theft of Equipment** | Inadvertent loss or removal by a third party of physical assets without consent. | 1 |
| **Malware** | Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. | 1 |
| **Phishing** | A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. | 2 |
| **Ransomware** | A type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. | 5 |
| **Spam** | Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. | 2 |
| **Unauthorized Access** | A person gains logical or physical access without permission to a network, system, application, data, or other resource | 2 |
| **Virus** | A computer program that can copy itself and infect a computer without permission or knowledge of the user; may corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. | 2 |
| **Vulnerability** | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Note: The term weakness is synonymous for deficiency. Weakness may result in security and/or privacy risks. | 2 |

***Sources:***


1. Law Insider, *Legal Definitions Dictionary*, https://www.lawinsider.com/dictionary
2. National Institute of Standards and Technology – U.S. Department of Commerce, *Computer Security Resource Center*, https://csrc.nist.gov/glossary
3. Federal Bureau of Investigation, *How We Can Help You: Business Email Compromise,* https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise
4. *Termly's Legal Dictionary,* https://termly.io/legal-dictionary/
5. National Institute of Standards and Technology – U.S. Department of Commerce, *Small Business Cybersecurity Corner: Ransomware,* https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware#:~:text=Ransomware%20is%20a%20type%20of,file%20from%20an%20external%20website

## Appendix C

## Complete List of Cybersecurity Incidents Reported to Arkansas Legislative Audit by a Public Entity For the Period July 1, 2024 through June 30, 2025

| Entity Type (Note 1) | Incident Type | # of Days Between Incident and Detection Dates | Current Status (Notes 2 and 3) |
|---|---|---|---|
| Higher Education | Breach of Confidentiality | 810 | Resolved |
| State Agency | Breach of Confidentiality | 803 | Resolved |
| Higher Education | Unauthorized Access | 784 | Resolved |
| School District | Malware Attack | 183 | Resolved |
| School District | Fraudulent Transaction | 112 | Resolved |
| School District | Malware Attack | 95 | Resolved |
| County | Fraudulent Transaction | 77 | Resolved |
| School District | Fraudulent Transaction | 73 | Resolved |
| County | Fraudulent Transaction | 71 | Resolved |
| School District | Fraudulent Transaction | 62 | Resolved |
| School District | Fraudulent Transaction | 53 | Under Investigation |
| School District | Business Email Compromise | 52 | Resolved |
| School District | Business Email Compromise | 43 | Resolved |
| School District | Fraudulent Transaction | 33 | Under Investigation |
| School District | Fraudulent Transaction | 33 | Resolved |
| School District | Business Email Compromise | 32 | Under Investigation |
| Community College | Fraudulent Transaction | 30 | Resolved |
| State Agency | Fraudulent Transaction | 28 | Resolved |
| School District | Fraudulent Transaction | 28 | Resolved |
| Community College | Unauthorized Access | 27 | Resolved |
| School District | Fraudulent Transaction | 25 | Resolved |
| County | Fraudulent Transaction | 24 | Resolved |
| School District | Fraudulent Transaction | 20 | Resolved |
| Municipality | Unauthorized Access | 19 | Resolved |
| School District | Fraudulent Transaction | 19 | Resolved |
| Higher Education | Unauthorized Access | 19 | Resolved |
| School District | Fraudulent Transaction | 19 | Under Investigation |
| School District | Fraudulent Transaction | 17 | Resolved |
| County | Fraudulent Transaction | 15 | Resolved |
| County | Fraudulent Transaction | 14 | Resolved |
| School District | Business Email Compromise | 12 | Resolved |
| County | Business Email Compromise | 12 | Under Investigation |
| Municipality | Fraudulent Transaction | 12 | Under Investigation |
| School District | Fraudulent Transaction | 11 | Resolved |
| School District | Unauthorized Access | 10 | Resolved |
| School District | Fraudulent Transaction | 10 | Resolved |
| State Agency | Spam or Phishing Attack | 9 | Resolved |
| School District | Unauthorized Access | 8 | Resolved |
| School District | Spam or Phishing Attack | 7 | Under Investigation |
| Higher Education | Breach of Confidentiality | 6 | Resolved |
| Higher Education | Unauthorized Access | 5 | Resolved |

## Appendix C (Continued)

| Entity Type (Note 1) | Incident Type | # of Days Between Incident and Detection Dates | Current Status (Notes 2 and 3) |
|---|---|---|---|
| Municipality | Spam or Phishing Attack | 5 | Resolved |
| School District | Spam or Phishing Attack | 5 | Under Investigation |
| Municipality | Business Email Compromise | 5 | Under Investigation |
| Higher Education | Unauthorized Access | 4 | Resolved |
| School District | Spam or Phishing Attack | 4 | Resolved |
| School District | Spam or Phishing Attack | 4 | Resolved |
| School District | Spam or Phishing Attack | 4 | Resolved |
| Municipality | Business Email Compromise | 3 | Resolved |
| State Agency | Unauthorized Access | 3 | Resolved |
| School District | Unauthorized Access | 3 | Resolved |
| School District | Fraudulent Transaction | 3 | Resolved |
| Higher Education | Spam or Phishing Attack | 3 | Resolved |
| School District | Fraudulent Transaction | 3 | Resolved |
| School District | Breach of Confidentiality | 3 | Resolved |
| School District | Spam or Phishing Attack | 3 | Resolved |
| County | Fraudulent Transaction | 3 | Under Investigation |
| County | Fraudulent Transaction | 2 | Resolved |
| Higher Education | Malware Attack | 2 | Resolved |
| County | Fraudulent Transaction | 2 | Resolved |
| School District | Fraudulent Transaction | 2 | Resolved |
| School District | Fraudulent Transaction | 2 | Resolved |
| Municipality | Fraudulent Transaction | 2 | Resolved |
| School District | Unauthorized Access | 1 | Resolved |
| Municipality | Fraudulent Transaction | 1 | Resolved |
| Higher Education | Spam or Phishing Attack | 1 | Resolved |
| Higher Education | Spam or Phishing Attack | 1 | Resolved |
| Higher Education | Unauthorized Access | 1 | Resolved |
| County | Fraudulent Transaction | 1 | Under Investigation |
| Higher Education | Breach of Confidentiality | 1 | Resolved |
| Higher Education | Unauthorized Access | 1 | Resolved |
| County | Fraudulent Transaction | 1 | Resolved |
| Higher Education | Unauthorized Access | 1 | Resolved |
| School District | Fraudulent Transaction | 1 | Resolved |
| Higher Education | Unauthorized Access | 1 | Resolved |
| Community College | Fraudulent Transaction | 1 | Resolved |
| School District | Spam or Phishing Attack | 1 | Resolved |
| School District | Spam or Phishing Attack | 1 | Resolved |
| Higher Education | Unauthorized Access | 1 | Resolved |
| School District | Business Email Compromise | 1 | Resolved |
| School District | Fraudulent Transaction | 1 | Resolved |
| County | Fraudulent Transaction | 1 | Resolved |
| County | Ransomware | 1 | Under Investigation |
| School District | Spam or Phishing Attack | 1 | Resolved |
| Higher Education | Spam or Phishing Attack | 1 | Resolved |
| School District | Business Email Compromise | 1 | Resolved |
| State Agency | Unauthorized Access | 1 | Resolved |
| School District | Spam or Phishing Attack | 1 | Resolved |
| School District | Spam or Phishing Attack | 1 | Resolved |
| School District | Ransomware | 1 | Under Investigation |

## Appendix C (Continued)

| Entity Type (Note 1) | Incident Type | # of Days Between Incident and Detection Dates | Current Status (Notes 2 and 3) |
|---|---|---|---|
| School District | Unauthorized Access | 1 | Under Investigation |
| County | Fraudulent Transaction | 0 | Resolved |
| State Agency | Business Email Compromise | 0 | Resolved |
| School District | Business Email Compromise | 0 | Resolved |
| Higher Education | Spam or Phishing Attack | 0 | Resolved |
| Community College | Ransomware | 0 | Resolved |
| School District | Fraudulent Transaction | 0 | Resolved |
| Municipality | Unauthorized Access | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Community College | Unauthorized Access | 0 | Resolved |
| County | Business Email Compromise | 0 | Resolved |
| Municipality | Business Email Compromise | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| State Agency | Cross-Site Scripting | 0 | Resolved |
| County | Spam or Phishing Attack | 0 | Resolved |
| County | Fraudulent Transaction | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Business Email Compromise | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| County | Business Email Compromise | 0 | Resolved |
| State Agency | Unauthorized Access | 0 | Resolved |
| Municipality | Unauthorized Access | 0 | Resolved |
| School District | Loss or Theft of Equipment | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Business Email Compromise | 0 | Resolved |
| School District | Business Email Compromise | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Under Investigation |
| Municipality | Fraudulent Transaction | 0 | Resolved |
| School District | Business Email Compromise | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Community College | Ransomware | 0 | Under Investigation |
| Higher Education | Business Email Compromise | 0 | Resolved |
| Municipality | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |

| Entity Type (Note 1) | Incident Type | # of Days Between Incident and Detection Dates | Current Status (Notes 2 and 3) |
|---|---|---|---|
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Breach of Confidentiality | 0 | Under Investigation |
| Municipality | Breach of Confidentiality | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| State Agency | Unauthorized Access | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| County | Brute Force Attack | 0 | Resolved |
| Community College | Malware Attack | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| School District | Business Email Compromise | 0 | Resolved |
| School District | Ransomware | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| School District | Fraudulent Transaction | 0 | Resolved |
| County | Ransomware | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| School District | Unauthorized Access | 0 | Resolved |
| Municipality | Fraudulent Transaction | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| County | Fraudulent Transaction | 0 | Under Investigation |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Municipality | Unauthorized Access | 0 | Resolved |
| State Agency | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Spam or Phishing Attack | 0 | Resolved |
| Municipality | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Under Investigation |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Municipality | Fraudulent Transaction | 0 | Resolved |
| School District | Fraudulent Transaction | 0 | Resolved |
| Higher Education | Malware Attack | 0 | Resolved |
| School District | Unauthorized Access | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| State Agency | Unauthorized Access | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Spam or Phishing Attack | 0 | Resolved |
| County | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Unauthorized Access | 0 | Resolved |
| Higher Education | Spam or Phishing Attack | 0 | Resolved |
| School District | Business Email Compromise | 0 | Resolved |
| State Agency | Unauthorized Access | 0 | Resolved |
| State Agency | Spam or Phishing Attack | 0 | Under Investigation |

| Entity Type (Note 1) | Incident Type | # of Days Between Incident and Detection Dates | Current Status (Notes 2 and 3) |
|---|---|---|---|
| State Agency | Fraudulent Transaction | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Municipality | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Municipality | Ransomware | 0 | Resolved |
| County | Ransomware | 0 | Under Investigation |
| County | Unauthorized Access | 0 | Under Investigation |
| Municipality | Fraudulent Transaction | 0 | Resolved |
| School District | Malware Attack | 0 | Under Investigation |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Unauthorized Access | 0 | Under Investigation |
| School District | Breach of Confidentiality | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| School District | Business Email Compromise | 0 | Resolved |
| Higher Education | Ransomware | 0 | Resolved |
| State Agency | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Community College | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| Higher Education | Unauthorized Access | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |
| School District | Spam or Phishing Attack | 0 | Resolved |

**Note 1:** Cybersecurity incidents reported may have occurred on the entity level or with an information system maintained by a contractual provider or another computer-related service provider.

**Note 2:** A public entity shall provide regular updates of the security incidents to ALA until the investigation of the security incident is closed.

**Note 3:** Ark. Code. Ann. § 10-4-429 states that a report, update, notification, or list created or maintained under this section is exempt as a security function under Ark. Code Ann. § 25-19-105(b)(11).

***Source**: Incident reports submitted by public entities (unaudited by Arkansas Legislative Audit)*

## Appendix D

## List of Cybersecurity Incidents Reported to Arkansas Legislative Audit By Entity Type For the Period July 1, 2024 through June 30, 2025

| Entity Type | Incident Type | Number of Incidents Reported |
|---|---|---|
| Community College | Fraudulent Transaction | 2 |
| | Malware Attack | 1 |
| | Ransomware | 2 |
| | Spam or Phishing Attack | 1 |
| | Unauthorized Access | 2 |
| County | Brute Force Attack | 1 |
| | Business Email Compromise | 3 |
| | Fraudulent Transaction | 14 |
| | Ransomware | 3 |
| | Spam or Phishing Attack | 2 |
| | Unauthorized Access | 1 |
| Higher Education | Breach of Confidentiality | 4 |
| | Business Email Compromise | 2 |
| | Malware Attack | 2 |
| | Ransomware | 1 |
| | Spam or Phishing Attack | 10 |
| | Unauthorized Access | 37 |
| Municipality | Breach of Confidentiality | 1 |
| | Business Email Compromise | 3 |
| | Fraudulent Transaction | 7 |
| | Ransomware | 1 |
| | Spam or Phishing Attack | 4 |
| | Unauthorized Access | 4 |
| School District | Breach of Confidentiality | 2 |
| | Business Email Compromise | 13 |
| | Fraudulent Transaction | 23 |
| | Loss or Theft of Equipment | 1 |
| | Malware Attack | 3 |
| | Ransomware | 2 |
| | Spam or Phishing Attack | 40 |
| | Unauthorized Access | 10 |
| State Agency | Breach of Confidentiality | 1 |
| | Business Email Compromise | 1 |
| | Cross-Site Scripting | 1 |
| | Fraudulent Transaction | 2 |
| | Spam or Phishing Attack | 3 |
| | Unauthorized Access | 7 |
| **Total** | | **217** |

***Source**: Incident reports submitted by public entities (unaudited by Arkansas Legislative Audit)*


LEGISLATIVE AUDIT
REGNAT POPULUS
MERCY
JUSTICE
ARKANSAS