Special Report

Arkansas Legislative Audit

Cybersecurity Incidents Reported by Public Entities

For the Period July 1, 2023 through June 30, 2024

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, 2023 through June 30, 2024. 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 monitoring 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: SPIS00424 Report Date: June 30, 2024

Legislative Update

During the Regular Session of 2023, the Arkansas General Assembly enacted two notable cybersecurity laws.

First, Act 846 of 2023 authorized formation of the Arkansas Cyber Response Board (Board), which is entrusted with overseeing the Arkansas Self-Funded Cyber Response Program. This initiative provides protection against covered, tangible losses or damages resulting from cyberattacks targeting counties, municipalities, and school districts within the State. The Board began receiving claims on July 1, 2024. The Board is also tasked with defining the minimum cybersecurity criteria to which governmental entities participating in the program must adhere. These entities shall have 12 months to comply with the minimum cybersecurity criteria established by this Act. Failure to meet these standards within the stipulated timeframe may result in a reduction in program coverage for the noncompliant entities.

Second, Act 504 of 2023 mandates that public entities develop two essential policies: one pertaining to the authorized use of technology resources and the other addressing cybersecurity concerns. This Act requires each state entity to "submit a cyber security policy for the state entity for approval to the State Cyber Security Office by October 1 of each even numbered year."

A technology resources policy is a set of guidelines, rules, and principles established by an organization or entity to govern the use, management, and maintenance of information assets (e.g., computer systems, networks, hardware, software, data, etc.). These policies are designed to ensure that technology resources are used securely, efficiently, and responsibly. Technology resources policies typically outline acceptable and unacceptable uses of technology; define security measures; address data privacy and confidentiality; and establish procedures for technology procurement, maintenance, and compliance. These policies are crucial for maintaining the integrity, security, and effectiveness of an organization's technological infrastructure while also promoting responsible and ethical technology usage among employees and stakeholders.

A cybersecurity policy is a comprehensive set of guidelines and procedures developed by an organization or entity to safeguard its digital assets, information systems, and data from various cyber threats and attacks. This policy outlines the organization's strategies, best practices, and protocols to prevent, detect, respond to, and recover from cybersecurity incidents.

RESULTS OF REVIEW

Summary of Cybersecurity Incidents Reported

During the period July 1, 2023 through June 30, 2024, 132 cybersecurity incidents were reported to ALA by 71 public entities at all levels of state government. A complete list of these incidents is provided in **Appendix C**. Of the 132 incidents reported, 109 have been resolved, and 23 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, and 2024. **Exhibit II on page 3** charts the incidents reported in fiscal year 2024 based on the month in which they were reported to ALA.

Exhibit I

Cybersecurity Incidents Reported to Arkansas Legislative Audit by Incident Type For Fiscal Years 2022, 2023, and 2024

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

*The reporting period began on July 28, 2021.

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

Exhibit II

Cybersecurity Incidents
By Month Incident Was Reported to Arkansas Legislative Audit (ALA)
For the Period July 1, 2023 through June 30, 2024

	Month Reported to ALA												
	2023						2024						Incident Type Totals
Incident Type	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	
Breach of Confidentiality	4		1				1	3	1				10
Brute Force Attack											1		1
Business Email Compromise						3		1	1		2	2	9
Fraudulent Transaction	5	3	1	2	3	3	1	1	1	2	3	4	29
Loss or Theft of Equipment							1						1
Malware Attack	1	2		2		1		1	1				8
Ransomware			2		1			2				1	6
Spam or Phishing Attack	3	3	3	2	4	2	3	6	3	2	6	4	41
Unauthorized Access	3	1	4	6	3	1	4	3	2				27
Monthly Totals	**16**	**9**	**11**	**12**	**11**	**10**	**10**	**17**	**9**	**4**	**12**	**11**	**132**

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

Most Significant Cybersecurity Incidents

During the review period, a third-party software provider used by several Arkansas governmental entities experienced a breach that affected MOVEit, a file transfer service owned by Progress Software. Although Arkansas government entities were not directly breached, the attack affected organizations with which they interact, such as retirement systems, banks, and the National Student Clearinghouse, as well as organizations that used MOVEit to send files containing sensitive data belonging to Arkansas entities. The complete extent of this breach is still being investigated.

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**, 132 cybersecurity incidents were reported to ALA by 71 public entities. Of the 132 incidents reported, 109 have been resolved, and 23 remain under investigation, as shown in **Appendix C**.

During the Regular Session of 2023, the Arkansas General Assembly enacted two additional cybersecurity laws. Act 846 of 2023 authorized formation of the Arkansas Cyber Response Board to oversee the Arkansas Self-Funded Cyber Response Program, which provides protection against covered, tangible losses or damages resulting from cyberattacks targeting certain public entities. Additionally, Act 504 of 2023 requires public entities to develop policies pertaining to the authorized use of technology resources and addressing cybersecurity concerns. As noted on **page 2**, these laws are in various stages of implementation.

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 (ALA) by a Public Entity − For the Period July 1, 2023 through June 30, 2024

Appendix D: List of Cybersecurity Incidents Reported to Arkansas Legislative Audit − By Entity Type − For the Period July 1, 2023 through June 30, 2024

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
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
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.	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 (ALA) by a Public Entity For the Period July 1, 2023 through June 30, 2024

Entity Type		Incident Type	Number of Days Between Incident and Detection (Note 2)	Current Status (Notes 3 and 4)
Higher Education		Unauthorized Access	267	Resolved
School District	(Note 1)	Unauthorized Access	118	Resolved
County		Fraudulent Transaction	84	Under Investigation
County		Fraudulent Transaction	60	Under Investigation
County		Fraudulent Transaction	57	Resolved
School District		Business Email Compromise	42	Under Investigation
Higher Education	(Note 1)	Breach of Confidentiality	40	Resolved
School District		Spam or Phishing Attack	29	Resolved
School District		Unauthorized Access	25	Resolved
School District	(Note 1)	Unauthorized Access	21	Resolved
County		Fraudulent Transaction	23	Under Investigation
Technical College	(Note 1)	Breach of Confidentiality	20	Resolved
School District		Malware Attack	20	Resolved
Higher Education		Unauthorized Access	19	Resolved
State Agency		Spam or Phishing Attack	19	Under Investigation
Municipality		Fraudulent Transaction	18	Resolved
Higher Education		Unauthorized Access	17	Resolved
School District		Spam or Phishing Attack	15	Resolved
School District		Fraudulent Transaction	15	Resolved
State Agency	(Note 1)	Ransomware	15	Under Investigation
Municipality		Business Email Compromise	14	Under Investigation
School District		Spam or Phishing Attack	13	Resolved
Higher Education		Unauthorized Access	12	Resolved
School District		Business Email Compromise	12	Resolved
Higher Education		Spam or Phishing Attack	10	Resolved
Municipality		Fraudulent Transaction	9	Resolved
Municipality		Spam or Phishing Attack	8	Resolved
Community College		Fraudulent Transaction	7	Resolved
Higher Education		Malware Attack	7	Resolved
School District		Business Email Compromise	6	Under Investigation
School District		Fraudulent Transaction	6	Resolved
State Agency	(Note 1)	Unauthorized Access	4	Resolved
Community College		Unauthorized Access	4	Resolved
Higher Education		Spam or Phishing Attack	4	Resolved
School District		Loss or Theft of Equipment	3	Under Investigation
Higher Education		Ransomware	2	Resolved
Municipality		Unauthorized Access	2	Resolved
Higher Education	(Note 1)	Breach of Confidentiality	2	Under Investigation
Community College	(Note 1)	Breach of Confidentiality	1	Resolved
State Agency		Spam or Phishing Attack	1	Resolved
Higher Education		Unauthorized Access	1	Resolved
Higher Education		Unauthorized Access	1	Resolved
State Agency		Unauthorized Access	1	Resolved
Higher Education		Malware Attack	1	Resolved
County		Fraudulent Transaction	1	Resolved
School District		Unauthorized Access	1	Resolved
School District		Malware Attack	1	Resolved
County		Fraudulent Transaction	1	Under Investigation
Municipality		Business Email Compromise	1	Under Investigation
Technical College	(Note 1)	Breach of Confidentiality	0	Resolved
Technical College	(Note 1)	Breach of Confidentiality	0	Resolved
Municipality		Fraudulent Transaction	0	Under Investigation
Higher Education		Malware Attack	0	Resolved

Appendix C (Continued)

Entity Type		Incident Type	Number of Days Between Incident and Detection (Note 2)	Current Status (Notes 3 and 4)
County		Fraudulent Transaction	0	Resolved
School District		Fraudulent Transaction	0	Resolved
School District		Spam or Phishing Attack	0	Under Investigation
Higher Education		Unauthorized Access	0	Resolved
Technical College		Spam or Phishing Attack	0	Resolved
Higher Education		Unauthorized Access	0	Resolved
School District		Spam or Phishing Attack	0	Resolved
Higher Education	(Note 1)	Malware Attack	0	Resolved
County		Fraudulent Transaction	0	Resolved
Higher Education		Unauthorized Access	0	Resolved
Higher Education		Malware Attack	0	Resolved
School District		Spam or Phishing Attack	0	Resolved
School District		Fraudulent Transaction	0	Resolved
School District		Fraudulent Transaction	0	Under Investigation
School District		Spam or Phishing Attack	0	Resolved
State Agency		Ransomware	0	Under Investigation
Higher Education		Ransomware	0	Resolved
County	(Note 1)	Breach of Confidentiality	0	Resolved
County		Spam or Phishing Attack	0	Resolved
County		Fraudulent Transaction	0	Resolved
Higher Education		Spam or Phishing Attack	0	Resolved
School District		Unauthorized Access	0	Resolved
School District		Spam or Phishing Attack	0	Resolved
School District		Unauthorized Access	0	Resolved
County		Fraudulent Transaction	0	Resolved
State Agency		Unauthorized Access	0	Resolved
School District		Spam or Phishing Attack	0	Resolved
School District		Fraudulent Transaction	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		Spam or Phishing Attack	0	Resolved
Higher Education		Business Email Compromise	0	Resolved
School District		Spam or Phishing Attack	0	Resolved
School District		Spam or Phishing Attack	0	Resolved
School District		Fraudulent Transaction	0	Resolved
Municipality		Fraudulent Transaction	0	Under Investigation
School District		Fraudulent Transaction	0	Resolved
School District		Business Email Compromise	0	Resolved
Higher Education		Spam or Phishing Attack	0	Resolved
School District	(Note 1)	Breach of Confidentiality	0	Resolved
School District		Fraudulent Transaction	0	Resolved
Higher Education		Unauthorized Access	0	Resolved
Technical College		Unauthorized Access	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
School District		Malware Attack	0	Resolved
County	(Note 1)	Breach of Confidentiality	0	Resolved
School District		Unauthorized Access	0	Resolved
Higher Education		Spam or Phishing Attack	0	Resolved

Appendix C (Continued)

Entity Type		Incident Type	Number of Days Between Incident and Detection (Note 2)	Current Status (Notes 3 and 4)
School District		Ransomware	0	Under Investigation
Higher Education		Spam or Phishing Attack	0	Resolved
School District		Spam or Phishing Attack	0	Resolved
State Agency	(Note 1)	Breach of Confidentiality	0	Under Investigation
Higher Education		Spam or Phishing Attack	0	Resolved
County		Fraudulent Transaction	0	Resolved
School District		Business Email Compromise	0	Resolved
Higher Education		Spam or Phishing Attack	0	Resolved
Community College		Unauthorized Access	0	Resolved
School District		Spam or Phishing Attack	0	Resolved
Higher Education		Spam or Phishing Attack	0	Resolved
School District		Fraudulent Transaction	0	Under Investigation
School District		Fraudulent Transaction	0	Under Investigation
Higher Education		Spam or Phishing Attack	0	Resolved
Higher Education		Spam or Phishing Attack	0	Resolved
Community College		Spam or Phishing Attack	0	Resolved
State Agency		Brute Force Attack	0	Resolved
Higher Education		Spam or Phishing Attack	0	Resolved
Higher Education		Spam or Phishing Attack	0	Resolved
State Agency		Spam or Phishing Attack	0	Resolved
Municipality		Spam or Phishing Attack	0	Resolved
County		Fraudulent Transaction	0	Under Investigation
County		Fraudulent Transaction	0	Under Investigation
School District		Business Email Compromise	0	Resolved
County		Ransomware	0	Resolved
Higher Education		Spam or Phishing Attack	0	Resolved
Municipality		Spam or Phishing Attack	0	Resolved

Note 1: These entities reported that the cybersecurity incident occurred with an information system maintained by a contractual provider or another computer-related service provider. These include entities affected by the MOVEit/Progress Software breach.
Note 2: Calculated number of days between the date the security incident occurred and the date it was detected.
Note 3: A public entity shall provide regular updates of the security incidents to ALA until the investigation of the security incident is closed.
Note 4: 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, 2023 through June 30, 2024

Entity Type	Incident Type	Number of Incidents Reported
Community College	Breach of Confidentiality	1
	Fraudulent Transaction	1
	Spam or Phishing Attack	1
	Unauthorized Access	2
County	Breach of Confidentiality	2
	Fraudulent Transaction	13
	Ransomware	1
	Spam or Phishing Attack	1
Higher Education	Breach of Confidentiality	2
	Business Email Compromise	1
	Malware Attack	5
	Ransomware	2
	Spam or Phishing Attack	15
	Unauthorized Access	13
Municipality	Business Email Compromise	2
	Fraudulent Transaction	4
	Spam or Phishing Attack	3
	Unauthorized Access	1
School District	Breach of Confidentiality	1
	Business Email Compromise	6
	Fraudulent Transaction	11
	Loss or Theft of Equipment	1
	Malware Attack	3
	Ransomware	1
	Spam or Phishing Attack	17
	Unauthorized Access	7
State Agency	Breach of Confidentiality	1
	Brute Force Attack	1
	Ransomware	2
	Spam or Phishing Attack	3
	Unauthorized Access	3
Technical College	Breach of Confidentiality	3
	Spam or Phishing Attack	1
	Unauthorized Access	1
Total		**132**

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

THIS PAGE LEFT INTENTIONALLY BLANK


LEGISLATIVE AUDIT
REGNAT POPULUS
MERCY
JUSTICE
ARKANSAS