Cyber Timeline

what to expect during a cyber event

Purpose: *This document is meant to provide superintendents and other district administrators with a timeline of events and other considerations to use with their administrative teams in order to inform, discuss, and plan before a cyber event occurs.*

Below is an outline of the stages to expect during a data breach. Know that no two events are identical. Every event is unique in the equipment, configurations, and policies owned and operated by the district.

Stage 1 - Preparation: The DIS Field Tech Team and Cyber Threat Response Team collaboratively work to provide regular training opportunities for staff and District Technology Coordinators (DTC) throughout the year. These training sessions can serve as important planning opportunities so that districts are prepared to respond during and after an event. It is important that district and school leadership teams educate teachers and staff to recognize and report potential cyber threats. In doing so, user awareness increases and the likelihood of an event occurring decreases.

Stage 2 - Identification: When malicious activity is suspected, immediately follow these 3 simple steps found on the Cyber Incident Card. It is important that cyber events are reported within the first 24 hrs. The superintendent and the District Technology Coordinator (DTC) should be in constant communication and work together to restore district operations. A full list of cyber contacts and communications protocols can be found later in this document.

Stage 3 - Containment: The tech teams involved will first work to contain and isolate the attack. Containment may include but is not limited to shutting down the internet, limiting email communications, disconnecting routers, and disconnecting switches to keep malicious software from spreading to other machines, schools, or districts. Shutting down access to eSchool & eFinance is a possibility to protect students' information, staff's information, and other state assets. Members from the DIS Field Tech Team or Cyber Threat Response Team will pull logs from an infected machine to submit for analysis with MS-ISAC and/or FBI.

Stage 4 - Eradication: After the threat has been contained, tech teams will work together to neutralize or remove the threat. This may include but is not limited to adjusting firewall rules, resetting user passwords, installing patches, and reviewing email configurations.

Stage 5 - Recovery: From there, tech teams will work cooperatively together to scrub and rebuild the district's network and machines to restore operation. This usually takes 3 to 10 days of intense labor, depending on the size of the district and the number of devices needing to be reconfigured.

Note: *It is typical for threat actors to encrypt district devices, servers, stored data files, network configurations, and other critical systems to severely interrupt daily business operations. Once data and network drives have been encrypted, there is little anyone can do to unencrypt them. During this process, it is common for local data to be extracted to an offsite location controlled by adversaries. Once data has been extracted, it is unlikely that the stolen data can be retrieved. These actions are often followed by a ransom message requesting payment to provide encryption and/or retrieval of stolen data.*

Operational Considerations

what to expect from an operational standpoint

Considerations **during** an event…

- Have a plan for payroll and other business operations. External networks can be used (e.g., hotspots, nearby districts, local coop).
- Be prepared to provide appropriate communications to school board members, parents, and other stakeholders as needed. Involving legal advisors may be necessary depending on the type and amount of data that was compromised. Legal counsel is often an additional cost to the district.
- Create a log of events as they unfold. This will prove to be incredibly useful in post-incident activities, recording the due diligence of the district, and providing historical documentation for concerns that may resurface at a later date.

Considerations **after** an event…

- Make plans to debrief with the district's response team and revise the emergency response plan as needed. State and coop technology leaders are ready and willing to be thought partners in this process.

Other considerations…

- Even though cybercrime does not discriminate, it isn't uncommon for first-year superintendents and/or first-year District Technology Coordinators to be targeted or become victims of a cyber attack. District leaders who have made the investment to conduct a cybersecurity assessment have found it to be worthwhile. It is difficult to have the institutional knowledge needed to protect a network when new to the environment.
- Having top-level discussions on how to communicate and operate during a cyber attack can significantly reduce confusion, data loss, and recovery time. Conducting a tabletop drill with the administrative team is a good exercise to recreate some of these discussions more naturally. The Cyber Threat Response Team can work with any district and/or coop to facilitate a tabletop drill at no charge.
- It is important to appropriate funds in the event of an emergency. Cyber events may involve unexpected expenditures (e.g., legal fees, equipment, technology services, software licenses, overtime pay) that are necessary to recover and respond.

System Reconnections

what to expect when state systems are disconnected due to a cyber attack

If the severity of an attack threatens state assets (e.g., eSchool, eFinance) to the level at which a district is disconnected from state systems, district leaders can expect to receive additional requirements from leaders at ADE and DIS to get reconnected. This list is not intended to cause additional inconvenience during an already tumultuous time. The intent is to protect state assets that could have repercussions for everyone without careful consideration. The number of days listed for each of the requirements below is in addition to the 3 to 10 days it takes to scrub and rebuild. The actions listed here would be performed after the district is back online and requesting to reconnect.

The list below is not meant to be exhaustive. Threat attackers are constantly modifying their tactics which require new strategies to protect and prevent.

Requirements may include…

- Endpoint Detection and Response (EDR) software on district machines. EDR is an additional cost to the district. An EDR solution provides real-time monitoring and analytics on individual computers. (1-2 days)
- Provide evidence that a clean vulnerability scan was conducted. DIS will provide this service. (1-2 days)
- Conduct a penetration test with adequate results. Penetration testing is an additional cost to the district. (1-2 days)
- Implement actions and/or controls to prevent reoccurrence. (timeline varies)
- Implement multi-factor authentication (MFA) district-wide.
- Implement 90-day password reset rules.
- Provide a summary detailing points of compromise, a timeline of events and actions, and steps for eradication. The summary will need to be reviewed and approved by leaders at ADE and DIS. (1-2 days)

Note: *Timelines provided here are estimates to be used as planning considerations. Totals will differ but a district should be prepared to operate with limited internet connectivity for 3 to 5 days and without access to state systems for at least 2 weeks. It is important to think through all the systems that are impacted when the internet is down (e.g., phones, intercoms, cameras, HVAC systems). If there is evidence that the district network and/or machines are still infected or unprotected, expect timelines to be extended until mitigation is complete.*

Cyber Insurance Considerations

what to expect from cyber insurance

Cyber insurance is intended to support an organization from data loss and financial liability in the event of a cyber attack. Cyber insurance adoption is a growing trend among school districts across the nation. As cyber attacks increase, the cost of cyber insurance has continued to increase as with the minimum conditions needed to become insurable. This document is only intended to support district leaders who are considering cyber insurance as part of their business operations.

Cyber insurance may provide…

- cyber forensic investigators
- ransom negotiators
- legal counsel
- crisis management
- public relations support
- financial protections

Cyber insurance in practice…

- Cyber insurance does not guarantee a speedier recovery. Once a claim is filed, the district will need to follow the prescribed recommendations to retain coverage. These terms typically dictate the actions of the technology staff and district leadership. This often includes what information can and cannot be shared with the public and other districts. Onsite support provided by the Cyber Threat Response Team and/or DIS Field Tech Team may not be allowable.
- To become insurable, insurance companies will set minimum requirements to reduce the risk of a payout. Many of the suggestions found on the "Cyber Prevention & Recovery" page would also be minimum requirements for attaining cyber insurance.
- The general recommendation from law enforcement is for districts to not pay the ransom in the event of a ransomware attack. Paying bad actors for criminal activity can exacerbate the issue. It is not uncommon for cybercriminals to target an organization multiple times for multiple payouts.
- Requiring contracted vendors and other third parties who handle sensitive information to carry cyber insurance may provide the district an additional layer of assurance when little visibility is available into another organization's cyber posture.

Note: *There is not a one size fits all approach when it comes to cyber insurance. It is important to pay close attention to the terms and protections because not all coverage is equal.*

Cyber Prevention & Recovery

actionable steps to reduce the risk and recovery time

Like many emergency-related situations, the risk of a cyber event can never be reduced to zero. There are steps a district can take to reduce the risk of an attack and recover more speedily. Many of the actions listed below align with the recent requirements for reconnecting to state systems after an attack, 2022 Arkansas School Safety Commission Final Report, and K12 SIX Essential Cybersecurity Protections for the 2022-2023 School Year.

The list below is not meant to be exhaustive. Threat attackers are constantly modifying their tactics which require new strategies to protect and prevent. Classifications relating to the impact on users and implementation cost can be viewed in more detail using the embedded links at the end of each action.

Preventative actions…

- The damage of a cyber attack has a strong correlation to the speed at which the district can respond and recover. It is important to review the district's Continuity of Operations Plan (COOP) and include preparations for a cyber-related event. Line out contracts, legal services, emergency contacts, and other partners (e.g., Cyber Threat Response Team, nearby tech at a district, community partner) that can be turnkey in the event of an attack. Establishing agreements and making arrangements before a cyber event will save time and money. (4.4 Plan for Cyber Incidents)
- Recovery time is largely impacted by the availability of clean backups. Districts should practice the use of offsite backups and take time to test those backups periodically throughout the year. DIS provides an offsite backup service at a minimal cost. (4.2 Manage Sensitive Data)
- Penetration testing and vulnerability scans can be used as preventative measures and are free with the Cybersecurity and Infrastructure Security Agency (CISA) and soon through the Cyber Threat Response Team.
- Invest in Endpoint Detection and Response (EDR) software. (2.2 Apply Endpoint Protection)
- Implement multi-factor authentication (MFA). There is generally no additional cost to implementing MFA but there is a learning curve to take into consideration when rolling out. (3.1 Protect User Logins)
- Engage and promote security awareness regularly. This is at no cost but requires leadership support. A commitment to increasing security awareness can be as simple as including a brief tip or short video before faculty meetings. District leaders should also consider getting involved in the monthly reminders through DESE's Security Awareness Insider. Staff presents the biggest threat to the safety of a district's network by the links they click, sites they visit, and passwords they set. At the same time, the staff is also an organization's biggest asset in protecting a district from a future cyber attack by understanding the risks and how to be safe. (4.2 Train to Improve Cybersecurity Awareness)

Note: *The process of securing and protecting the district network is a continuous one. Districts should continuously assess, revise, and mature as part of the Plan-Do-Check model.*

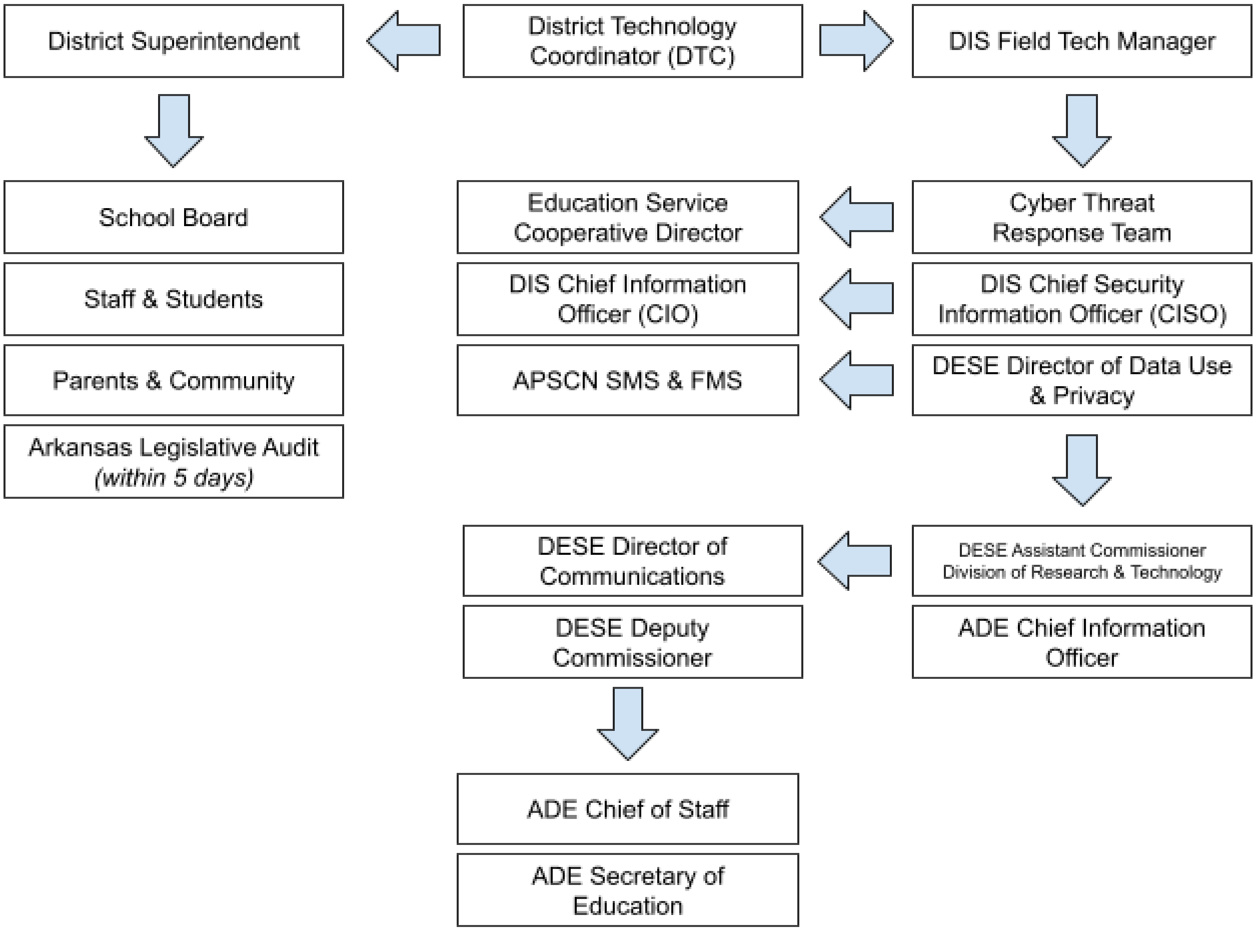
Cyber Contacts

below is a list of dedicated professionals that can be utilized in the event or prevention of a cyber attack

Name	Organization	Title	Phone	Email
Ray Girdler	Division of Elementary and Secondary Education (DESE)	Director of Data Use & Privacy	Office: (501)683-4230 Cell: (501)733-1802	ray.girdler@ade.arkansas.gov
Krissy Cross	Division of Information Systems (DIS)	DIS - APSCN LAN Support Team Manager	Office: (501)683-3637 Cell: (501)230-4741	kristina.cross@arkansas.gov
Evan Patrick	Southeast Co-op	Technology Coordinator/ Director of Arkansas' P-12 Cyber Threat Response Team	Cell: (870)304-6771	evan.patrick@searkcoop.com
Alan Floyd	Northcentral Co-op	Technology Coordinator/ Associate Director of Arkansas P-12 Cyber Threat Response Team	Cell: (870)373-0571	alan.floyd@northcentralcoop.org
Chad Johnson	Cybersecurity & Infrastructure Security Agency (CISA)	Cybersecurity Advisor (Arkansas)	Cell: (501)487-8086	chad.johnson@cisa.dhs.gov
Chris Carter	Federal Bureau of Investigation (FBI)	Special Agent	Office: (501)221-9100	lr_ctf@ic.fbi.gov
David Coles	Arkansas Legislative Audit	Deputy Legislative Auditor	Office: (501)683-8600 Ext: 1040	david.coles@arklegaudit.gov
Arijit Sarkar	Arkansas Department of Education (ADE)	Chief Information Officer	Office: (501)682-1524	arijit.sarkar@ade.arkansas.gov
Jonathan Askins	Division of Information Systems (DIS)	Director/Chief Technology Officer	Office: (501)682-4976	jonathan.askins@arkansas.gov
Gary Vance	Division of Information Systems (DIS)	Chief Information Security Officer	Office: (501)682-9437	gary.vance@arkansas.gov

Communication Protocols

below is a map of the communication protocols when cyber incidents are reported



District Technology Coordinator (DTC)

District Superintendent

School Board

Staff & Students

Parents & Community

Arkansas Legislative Audit *(within 5 days)*

DIS Field Tech Manager

Cyber Threat Response Team

DIS Chief Security Information Officer (CISO)

DESE Director of Data Use & Privacy

Education Service Cooperative Director

DIS Chief Information Officer (CIO)

APSCN SMS & FMS

DESE Assistant Commissioner Division of Research & Technology

ADE Chief Information Officer

DESE Director of Communications

DESE Deputy Commissioner

ADE Chief of Staff

ADE Secretary of Education

Cyber Resources

free resources for district planning and preparations

Implementing new policies, practices, and products can be costly. Before investing in paid services, districts are encouraged to explore resources that are currently available at no charge.

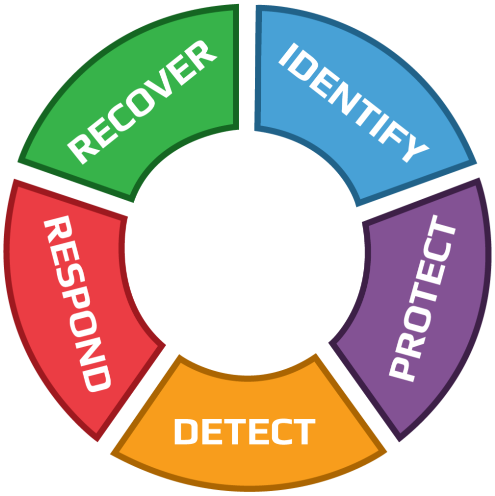
Cybersecurity & Infrastructure Security Agency (CISA)

CISA is an operational component of the Department of Homeland Security (DHS). CISA released its "Partnering to Safeguard K-12 Organizations from Cybersecurity Threats" report with a supporting toolkit for K-12 institutions to help them better protect against cybersecurity threats. The report provides recommendations and resources to help K-12 schools and school districts address systemic cybersecurity risks. It also provides insight into the current threat landscape specific to the K-12 community and offers simple steps school leaders can take to strengthen their cybersecurity efforts.

https://www.cisa.gov/partnering-safeguard-k-12-toolkit

National Institute of Standards and Technology (NIST)

NIST is part of the U.S. Department of Commerce. NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public. The NIST cybersecurity framework is widely considered to be the standard for building a cybersecurity program.



The NIST Cybersecurity Framework

https://www.nist.gov/cyberframework

PowerSchool

PowerSchool is the contracted provider for Arkansas' eSchoolPlus and eFinancePlus solutions. PowerSchool has compiled resources, K-12 Data Security and Privacy Resource Kit, to support data security and data privacy needs at the district level.

https://www.powerschool.com/data-security-and-privacy-resource-kit/

Criminal Justice Institute (CJI)

CJI is a University of Arkansas System campus. CJI offers a host of courses for district leaders, teachers, and technology professionals under their Cybersecurity Defense Initiative (CDI) program. CDI and its courses were developed under a cooperative agreement from the U.S. Department of Homeland Security/FEMA, National Training and Exercises Division.

https://www.cji.edu/cji-programs/cybersecurity-defense-initiative/

Division of Elementary & Secondary Education (DESE)

Under DESE's Division of Research and Technology, resources have been compiled to support Arkansas districts in responding to and preventing damage involving a cyber attack. Information for the Cyber Threat Response Team, Security Awareness, Privacy Awareness, and Social Media Awareness Campaign (SMACtalk) can all be found on the DESE Division of Research and Technology webpage. DESE works collaboratively with the coop technology coordinators from across the state to compile resources and provide regional support.

https://dese.ade.arkansas.gov/Offices/research-and-technology

Consortium for School Networking (CoSN)

CoSN is the premier membership organization designed to meet the needs of K12 education technology leaders. CoSN's resources support the entire IT team in a school system/district. CoSN offers a host of cybersecurity resources designed specifically for public schools.

https://www.cosn.org/edtech-topics/cybersecurity/

K12 Security Information eXchange (K12 SIX)

K12 SIX is a cyber threat information sharing community dedicated solely to the needs of U.S. primary and secondary education organizations. K12 SIX Essentials series establishes baseline cybersecurity standards for U.S. school districts and provides guidance and tools to support district implementation. K12 SIX recommended practices are designed to defend against the most common cyber threats facing school districts.

https://www.k12six.org/essentials-series

Center for Internet Security, Inc. (CIS)

CIS is globally recognized for providing best practices for securing IT systems and data. CIS also manages the Multi-State Information Sharing and Analysis Center (MS-ISAC). The mission of MS-ISAC is to improve the overall cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication.

https://www.cisecurity.org/