// FREE SCHOOL RESOURCE

K-12 Ransomware Tabletop Exercise

A realistic, discussion-based exercise for school and district incident-response teams

// WHAT THIS PACK PROVIDES

- A complete 60-90 minute ransomware scenario with timed injects.
- Facilitator guidance, expected actions and role-specific discussion questions.
- Attendance, evaluator, communications, reporting and ransom-decision worksheets.
- An action tracker and two-page after-action report for formal follow-through.
- References limited to official U.S. federal and state government sources.

// FOR SUPERINTENDENTS, SCHOOL LEADERS, IT, OPERATIONS, COMMUNICATIONS, FINANCE, LEGAL, HR AND STUDENT SERVICES

// START HERE

How to use this exercise

A practical exercise pack - not legal advice or a replacement for district policy

Exercise the plan before the incident.
CISA provides tabletop exercise packages so organizations can discuss how they would respond to cyber threats, and the U.S. Department of Education points schools toward drills, exercises and cybersecurity planning. This pack adapts that approach for smaller K-12 teams. [1][2][3]

Six operating principles

01 **Discussion, not simulation.** No production systems are touched. Participants talk through decisions using current plans and contacts.

02 **People and school operations first.** Protect student supervision, transportation, meals, medication, payroll and emergency communications.

03 **No-fault learning.** The aim is to find gaps before an attacker does, not to grade or embarrass individuals.

04 **State what you know.** Separate confirmed facts, assumptions, unknowns and decisions that require approval.

05 **Use real roles and channels.** Participants should follow the district's actual authority, insurance, legal and communications routes.

06 **Finish with owners and dates.** Every important gap becomes a tracked corrective action.

Use this pack in four ways

- ☐ Full 90-minute district exercise.
- ☐ Condensed 60-minute leadership session.
- ☐ School-level discussion before a district exercise.
- ☐ Annual validation of the Cyber Annex or incident plan.

Important. This is a planning resource, not legal advice or a replacement for district policy. State breach, education, public-records and ransom-reporting requirements vary.

// VERSION CONTROL

District / school: _____

Exercise owner: _____

Approved by: _____

Exercise date: _____

Next review: _____

// EXERCISE DESIGN

Objectives, participants and schedule

A 60-90 minute discussion-based exercise

Exercise objectives

- ☐ Recognize, declare and lead a significant cyber incident.
- ☐ Contain affected systems without destroying evidence.
- ☐ Maintain essential school and district operations.
- ☐ Coordinate legal, insurance, federal and state reporting.
- ☐ Communicate verified information to staff, families, boards and media.
- ☐ Identify improvements, owners, due dates and re-test needs.

Who should attend

Superintendent or designee, IT lead, operations, communications, finance, HR, legal/privacy, student services, school leadership and an evaluator/scribe.

Small district option: one person may hold more than one role, but decision authority should remain clear.

Invite as observers: cyber insurer, managed service provider, county emergency management or state cyber liaison, subject to confidentiality rules.

// 90-MINUTE RUN OF SHOW

TIME	ACTIVITY	FACILITATOR PURPOSE
0-10 min	Welcome, rules and baseline	Set a no-fault environment, confirm roles and explain how injects will be delivered.
10-25 min	Module 1 - Discovery	Test declaration, containment, leadership activation and opening decisions.
25-40 min	Module 2 - Operational disruption	Test continuity, technical coordination and out-of-band communications.
40-60 min	Module 3 - Data theft and ransom	Test reporting, privacy, insurance, legal review and ransom governance.
60-75 min	Module 4 - Public pressure and recovery	Test family/media communications, restoration priorities and secondary threats.
75-90 min	Hotwash and actions	Capture strengths, gaps, owners, due dates and the next exercise.

60-minute option

Use the core injects only, limit each module to 10 minutes, and reserve 10 minutes for the hotwash. Do not skip corrective-action ownership.

Success is observable

Participants identify authority, preserve facts and evidence, maintain essential services, use trusted reporting routes and assign measurable improvements.

// FACILITATOR SETUP

Prepare the exercise

Preparation protects the value and safety of the session

Seven to fourteen days before

- [ ] Name the facilitator, scribe/evaluator and exercise sponsor.
- [ ] Confirm participants and decision-makers.
- [ ] Review the incident plan, Cyber Annex, continuity plan and communications plan.
- [ ] Verify insurer, counsel, incident-response vendor and reporting contacts.
- [ ] Choose the 60- or 90-minute format and optional injects.

Twenty-four hours before

- [ ] Print role cards, injects, attendance and action tracker.
- [ ] Confirm room, remote access and a visible clock.
- [ ] Mark exercise materials "EXERCISE - NOT A REAL INCIDENT."
- [ ] Remove real passwords, student records and sensitive system details.

Ground rules to read aloud

1. Treat the scenario as plausible, but do not invent capabilities you do not have.
2. State who has authority to decide, approve and communicate.
3. Use current district procedures; flag missing or outdated procedures.
4. Do not use real student information, credentials or confidential network details.
5. The facilitator may pause or accelerate the exercise.
6. Real emergencies take priority. Say **"REAL-WORLD INCIDENT"** to stop the exercise.

Do not turn the exercise into

A technical troubleshooting contest, a blame session, a policy debate with no decision, or a presentation where participants never have to choose.

// FACILITATOR CONTACTS

ROLE	NAME	PHONE / OUT-OF-BAND CONTACT	BACKUP
Exercise sponsor			
Facilitator			
Scribe / evaluator			
Real-world emergency contact			

// SCENARIO

District profile and starting conditions

Fictional scenario - adapt only non-sensitive details

All organizations, people, systems and events in this scenario are fictional.
Adapt names and non-sensitive operating details, but keep the pressure points: small IT capacity, essential services, sensitive student data, uncertain backups and a fast-moving public narrative.

Pine Ridge Unified School District

2,600	340	4	4
students	staff	schools	IT staff

Environment. Cloud email and collaboration; Windows staff devices; student Chromebooks; on-premises identity, file and print services; cloud student-information and HR/payroll systems; networked phones, transportation and cafeteria systems.

Support. One managed-service provider assists after hours. The cyber insurance policy requires prompt notice and may require approved counsel and incident-response vendors.

Backups. Nightly backups and a weekly isolated copy are configured. The last documented full restore test was four months ago.

Planning. The cyber incident plan was updated 18 months ago. The emergency operations plan mentions technology disruption but does not name restoration priorities.

Operating context

Day: Monday in October.

Time: 6:35 a.m., before staff arrival.

Pressure: Payroll files close today. State testing begins next week. A school board meeting is scheduled tonight.

Weather: Heavy rain; transportation changes are likely.

Public expectation: Schools are scheduled to open normally.

Facilitator: Ask participants what additional facts they need, but only provide information contained in later injects unless the question tests a real district procedure.

// BASELINE INFORMATION PARTICIPANTS MAY ASSUME

KNOWN	NOT YET KNOWN
Cloud email is working. Some on-premises systems are slow. IT staff are on site or reachable. District leadership can use personal phones for approved out-of-band calls.	Initial entry point, number of affected systems, whether data left the network, whether backups are clean, attacker identity, legal notification triggers and time to restore.

// PEOPLE

Roles and attendance

Assign authority before the first inject

Core roles

ROLE	EXERCISE RESPONSIBILITY
Incident executive	Declares district incident, sets priorities, approves major operational and public decisions.
Incident lead / coordinator	Maintains common operating picture, actions, owners, time stamps and briefings.
IT / security lead	Explains containment, evidence, vendor coordination, restoration and technical uncertainty.
Operations / school leadership	Protects supervision, transportation, meals, facilities, attendance and school opening.
Communications	Drafts staff, family, board and media messages using verified facts.
Legal / privacy / HR	Reviews authority, student and employee data, state law, records and notification.
Finance / insurance	Notifies insurer, protects payments, tracks cost and supports ransom governance.
Scribe / evaluator	Records decisions, gaps, strengths, unresolved questions and corrective actions.

Role assignment

Incident executive: _____

Incident lead: _____

IT / security: _____

Operations: _____

Communications: _____

Legal / privacy: _____

Finance / insurance: _____

Scribe / evaluator: _____

// ATTENDANCE SHEET

NAME	TITLE / ORGANIZATION	EXERCISE ROLE	EMAIL OR INITIALS

// MODULE 1

Discovery and declaration

Deliver injects at 0, 7 and 12 minutes

Module objective:
Recognize a major incident, establish leadership, protect essential services, begin containment and preserve evidence.

0 MIN	**Help desk alert.** Three staff members report that shared files now have unfamiliar extensions. Two devices display a ransom note. Endpoint protection quarantined a suspicious process on one device. A file server is unusually slow.
7 MIN	**Identity warning.** The IT lead finds a privileged account used overnight from an unfamiliar internet address. Several failed administrator logins continue. The district does not yet know whether the account is still active.
12 MIN	**Opening pressure.** A principal asks whether schools should open. Staff need printing and shared drives. Heavy rain may require bus-route changes.

Discussion questions

> Who declares an incident, and at what severity?

> What systems or accounts should be isolated first?

> What must be preserved before rebooting, wiping or rebuilding?

> How will leaders communicate if district email or identity becomes unreliable?

> What information does the superintendent need in the first briefing?

> What operational conditions would change the decision to open schools?

Decisions to record

Incident level: _____

Incident executive: _____

Incident lead: _____

Systems/accounts isolated:

_____

Opening decision owner: _____

Next briefing time: _____

Out-of-band channel: _____

Facilitator watch item: Participants should not assume that rebooting, reimaging or shutting down every device is harmless. Ask who authorizes destructive actions and how evidence will be protected.

// MODULE 2

Containment and operational disruption

Deliver injects at 15, 21 and 27 minutes

Module objective:
Contain spread, maintain school operations and coordinate technical, leadership and vendor actions.

15 MIN	**Service disruption.** File shares, printing and several on-premises applications are unavailable. Bus routing and cafeteria point-of-sale systems cannot retrieve current data. Cloud email still works, but desk phones are intermittent.
21 MIN	**Scope expands.** Endpoint alerts appear in two schools. The managed-service provider can assist remotely but asks whether its access should be disabled or preserved for investigation.
27 MIN	**Ransom note.** A note appears on multiple servers. It claims files were encrypted after data was copied and gives the district 24 hours to make contact.

Discussion questions

> Which network segments, remote access paths and privileged accounts are contained?

> Who contacts the managed-service provider and cyber insurer?

> How will buses, meals, attendance, medication and payroll continue manually?

> What systems are highest priority for safe restoration?

> How often will the incident team brief school leaders?

> What facts support or contradict the claim that data was stolen?

Continuity priorities

- [ ] Student supervision and emergency contacts
- [ ] Transportation and route changes
- [ ] Meals and point-of-sale alternatives
- [ ] Health, medication and special services
- [ ] Attendance, payroll and vendor payments

Optional inject. The cloud email provider reports no compromise. Ask whether the district will continue using email and what contingency is needed if identity systems fail.

// MODULE 3

Data theft and ransom demand

Deliver injects at 33, 39 and 45 minutes

Module objective:
Address suspected data theft, ransom governance, privacy, insurance, evidence and federal/state reporting.

33 MIN	**Data sample.** A monitoring service finds a leak-site post naming the district. The sample appears to include a student special-education record, a health document and part of a staff tax form.
39 MIN	**Insurance conditions.** The insurer says it must be notified promptly and asks the district not to retain outside counsel, negotiate or restore systems until approved panel resources are discussed.
45 MIN	**Demand.** The actor demands $350,000 in cryptocurrency and threatens to publish all copied data. The note offers to decrypt two files as proof.

Discussion questions

> Who verifies whether the sample is authentic and what data population may be affected?

> What are the district's federal, state, insurer and contractual reporting steps?

> Who is authorized to communicate with the actor, if anyone?

> What legal, law-enforcement, insurance and board approvals govern any ransom decision?

> How will the district preserve the ransom note, sample files and communications?

> What can be said to affected people before scope is confirmed?

Ransom reality

The FBI does not support paying a ransom. Payment does not guarantee restoration or deletion and may encourage further crime. Any decision requires authorized legal, insurance, law-enforcement and leadership review. [4][5]

Reporting prompt

Identify who will report to CISA, the local FBI field office and IC3, and who will determine state-specific deadlines.

// MODULE 4

Communications and recovery

Deliver injects at 52, 58, 64 and 69 minutes

Module objective:
Manage public pressure, make restoration choices, communicate uncertainty and prepare for secondary attacks.

52 MIN	**Recovery estimate.** The backup administrator finds an isolated copy believed to be clean, but it is five days old. A full prioritized restore may take 36-72 hours. Some transportation and payroll changes would need manual reconstruction.
58 MIN	**Public narrative.** A student posts a screenshot claiming "all student Social Security numbers were stolen." A local reporter asks for confirmation within 20 minutes. The claim is not verified.
64 MIN	**Leadership pressure.** A board member posts that the district has "lost everything" and asks why families were not notified immediately. The actor emails the board directly.
69 MIN	**Secondary threat.** Staff receive messages pretending to be district IT and asking them to "revalidate" passwords through a link.

Discussion questions

> What is restored first, and what evidence proves the environment is safe?

> How will the district handle the five-day data gap?

> What holding statement can be issued now without speculation?

> Who corrects unauthorized board or staff statements?

> How will staff receive trusted password-reset instructions?

> What monitoring and heightened controls continue after restoration?

End-state decisions

School status: _____

First restore priority: _____

Family update time: _____

Board briefing owner: _____

Password-reset channel: _____

Next operational review: _____

Expected actions - Modules 1 and 2

Use prompts to expose process gaps, not to give a lecture

Module 1 - expected actions

- ☐ Declare an incident and name one incident executive and one coordinator.
- ☐ Use an approved out-of-band channel if identity or email may be compromised.
- ☐ Isolate affected systems and privileged accounts in a controlled manner.
- ☐ Preserve logs, ransom notes, alerts, times and administrator activity.
- ☐ Set an opening/closure decision process based on essential services and safety.
- ☐ Set a briefing rhythm and a single source of verified facts.

Module 2 - expected actions

- ☐ Identify critical systems and manual continuity procedures.
- ☐ Coordinate with the managed-service provider without expanding compromise.
- ☐ Notify the cyber insurer and follow approved vendor/ counsel conditions.
- ☐ Protect backups and prevent them from being connected to a compromised environment.
- ☐ Determine initial scope while acknowledging uncertainty.
- ☐ Document containment decisions and who approved them.

// PROMPTS WHEN DISCUSSION STALLS

ASK	WHY IT MATTERS
"Who has authority to make that decision at 6:45 a.m.?"	Exposes unclear delegations and after-hours authority.
"What would you do if district email stopped working now?"	Tests trusted, out-of-band communications.
"Which service must be restored first, and who agreed that before today?"	Tests documented business priorities rather than IT assumptions.
"What evidence would be lost by that action?"	Discourages premature wiping, rebooting or rebuilding.
"What do we know, what do we think, and what remains unknown?"	Improves briefings and prevents unsupported public claims.

Common failure: Every decision routes through one overloaded IT person while leadership waits for technical certainty that may not arrive.

Good outcome: Leadership manages priorities and communications while technical teams contain, preserve and assess.

Expected actions - Modules 3 and 4

Federal reporting and state review belong inside the exercise

Module 3 - expected actions

- ☐ Treat the leak sample as evidence and limit unnecessary access or distribution.
- ☐ Engage authorized counsel, insurer and incident-response resources.
- ☐ Report to CISA, local FBI and IC3 through official channels.
- ☐ Identify state education, cyber and breach-notification requirements.
- ☐ Establish who may communicate with the actor and preserve all contact.
- ☐ Use a documented ransom-decision process; do not imply payment guarantees recovery.

Module 4 - expected actions

- ☐ Validate clean backups and rebuild through a controlled restoration sequence.
- ☐ Prioritize safety and operations, not merely the easiest system to restore.
- ☐ Issue a verified holding statement and define the next update time.
- ☐ Correct misinformation without repeating unverified claims as fact.
- ☐ Use trusted reset instructions and warn staff about follow-on phishing.
- ☐ Continue monitoring, evidence retention and after-action work after service returns.

// OPTIONAL BRANCHES

IF PARTICIPANTS...	ADD THIS INJECT
Contain too easily	A vendor remote-support account is still active and its owner cannot be reached for 20 minutes.
Assume backups solve everything	The last clean restore point is ten days old and the backup console used the compromised administrator account.
Communicate too confidently	A second data sample contradicts the first estimate of affected records.
Ignore school operations	Medication records are unavailable and a student requires a time-sensitive dose under the district's normal process.
Rush toward payment	The actor changes the wallet address and claims the deadline was shortened because the district contacted law enforcement.

No single perfect answer. Evaluate whether participants use lawful authority, verified information, documented priorities, trusted partners and reversible decisions where possible.

// DISCUSSION

Questions by role

Use the questions to test decisions, not technical trivia

Superintendent / incident executive

> What must be decided now, and what can wait?

> Who has delegated authority after hours?

> What conditions determine school opening or closure?

Communications

> What is confirmed, unknown and being done?

> Who approves staff, family, board and media messages?

> When is the next update promised?

IT / security

> What can be isolated without blocking evidence collection?

> How are privileged accounts and backups protected?

> What proves systems are safe to restore?

Legal / privacy / HR

> What data and populations may be affected?

> Which state, FERPA, contract and records rules require review?

> How is sensitive evidence shared on a minimum-necessary basis?

Operations / principals

> Which functions can operate manually, for how long?

> How are transportation, meals, health and attendance protected?

> How are school leaders briefed consistently?

Finance / insurance

> What notices and approvals does the policy require?

> How are payroll, banking changes and fraud risks controlled?

> Who tracks costs and preserves coverage documentation?

// WHOLE-TEAM QUESTIONS

QUESTION	ANSWER / GAP
Where is the incident plan stored if the network is unavailable?	
What is the district's approved out-of-band communication method?	
Which three systems are restored first, in order?	
Who owns state reporting and who is the backup?	
When was the last full restore test, and what did it prove?	

// DECISION WORKSHEET

Ransom governance

Document authority, advice, alternatives and uncertainty

This worksheet is a decision-governance aid, not a recommendation to pay.
The FBI does not support paying ransomware demands. Payment does not guarantee data recovery or deletion. Contact law enforcement and use authorized legal, insurance and leadership review. [5]

Decision gates

- ☐ Incident executive and decision authority confirmed.
- ☐ Local FBI / IC3 and CISA reporting completed or underway.
- ☐ Cyber insurer and approved counsel engaged.
- ☐ Lawful authority, sanctions and policy implications reviewed.
- ☐ Backup viability and realistic restoration time assessed.
- ☐ Evidence of exfiltration and affected data assessed.
- ☐ Operational, safety, financial and reputational impacts documented.
- ☐ Board or governing-body requirements confirmed.

Questions the record should answer

What essential services are unavailable?

What restoration options exist without payment?

What uncertainties remain?

Who provided legal, insurance and law-enforcement advice?

What decision was made and why?

// DECISION RECORD

FIELD	ENTRY
Decision	
Authority / approval	
Date and time	
Conditions / assumptions	
Next review point	

// COMMUNICATIONS

Draft verified messages

Accurate, timely and coordinated - without speculation

Holding statement framework

What happened: We are responding to a cybersecurity incident affecting certain district technology services.

What we are doing: We activated our incident-response procedures and are working with specialized partners and law enforcement.

Operational status:

_____

What is not yet known:

_____

Next update: We expect to provide another update by _____.

Do not promise: that no data was accessed, that all data was stolen, that systems are safe, or that a specific restoration time is guaranteed unless verified.

Message approval

Drafted by: _____

Fact-check owner: _____

Legal/privacy review: _____

Approved by: _____

Channels: _____

Publication time: _____

Next update owner: _____

// DRAFTING EXERCISE

AUDIENCE	WHAT THEY NEED TO KNOW	MESSAGE / OWNER / CHANNEL
Staff	How to work safely, where to get instructions, phishing warning, what not to do.	
Families	School status, services affected, verified privacy facts, support and next update.	
School board	Known impact, major decisions, legal/insurance posture, public message and risks.	
Media / public	Verified facts, operational status, response partners and update schedule.	

Exercise inject: A fake "district IT" password-reset message is spreading. Draft a two-sentence warning that tells staff exactly where authentic instructions will appear.

Federal and state worksheet

Examples are not exhaustive - verify current state and district requirements

Federal reporting routes

CISA: Report online at cisa.gov/report or call 1-844-SAY-CISA (1-844-729-2472).

FBI: Contact the local FBI field office for cyber-criminal activity and investigative support.

IC3: File a ransomware complaint at ic3.gov and preserve the complaint/reference details.

U.S. Department of Education: Use Student Privacy Policy Office resources to assess education-record and privacy response issues.

CISA and FBI guidance emphasizes prompt reporting, evidence preservation, coordinated response and accurate information sharing. [4][5][6]

State examples - verify locally

Texas: DIR states local governments must report security incidents within 48 hours; school districts and charter schools use the Local Government Incident Report. [8]

New York: School districts are within the state definition of municipal corporation. Report a cyber incident or ransom demand within 72 hours; ransom payments have additional 24-hour and 30-day reporting. [9]

Georgia: GEMA/HS provides the state cyber incident reporting system and states Georgia agencies and utilities are required to report under state law. Verify district applicability and local process. [10]

California: State law governs resident breach notice; when a notice is required for more than 500 California residents, a sample notice must be submitted to the Attorney General. [11]

// DISTRICT REPORTING WORKSHEET

ROUTE	TRIGGER / DEADLINE	OWNER / BACKUP	CONTACT / CONFIRMATION
CISA			
FBI / IC3			
State cyber agency			
State education agency			
Attorney General / breach notice			
Insurer / vendor / contract			

Scorecard and observation notes

Scores require observable evidence

Evaluator method:
Rate what participants demonstrated during the exercise, not what the district hopes its plan would do. Record evidence and avoid unsupported scores.

CAPABILITY	1	2	3	4	5	OBSERVATION / EVIDENCE
Leadership and incident declaration						
Common operating picture and briefings						
Containment and privileged-account control						
Evidence preservation and documentation						
Continuity of essential school operations						
Legal, privacy, insurance and reporting						
Staff, family, board and media communications						
Backup validation and recovery priorities						
Ransom-decision governance						
Corrective-action ownership						

Rating scale

1: Not demonstrated

2: Major gaps / unclear ownership

3: Partly effective / inconsistent

4: Effective with minor improvements

5: Clear, timely, documented and coordinated

Hotwash prompts

> What worked better than expected?

> Where did authority or information stall?

> Which plan, contact or technical control was missing?

> What must be fixed in 30 days?

> What must be re-exercised?

// IMPROVEMENT PLAN

Corrective-action tracker

A finding without an owner and due date is not an improvement

Convert every material gap into an improvement action.
Actions should be specific, owned, time-bound and supported by evidence of completion. Avoid entries such as "improve security" without a measurable result.

GAP / OBSERVATION	CORRECTIVE ACTION	OWNER	PRIORITY	DUE DATE	EVIDENCE / STATUS

Priority guide

Critical: life safety, immediate compromise, legal deadline or inability to operate.

High: material control or coordination gap likely to worsen impact.

Medium: process improvement with a workable interim control.

Low: documentation, usability or efficiency improvement.

Review rhythm

30-day review: _____

90-day review: _____

Plan update owner: _____

Re-exercise date: _____

Board / leadership report: _____

// AFTER-ACTION REPORT

AAR - summary and findings

Complete while observations are fresh

Exercise overview

District / school: _____

Exercise date: _____

Location / format: _____

Facilitator: _____

Evaluator / scribe: _____

Number of participants: _____

Exercise length: _____

Overall assessment

Overall rating (1-5): _____

Plans tested: _____

Primary objective met? _____

Immediate issue requiring escalation? _____

Next leadership review: _____

// EXECUTIVE SUMMARY

Summarize the scenario, major decisions, operational consequences and overall readiness. Focus on facts observed during the exercise.

// STRENGTHS

List capabilities that were timely, coordinated, documented and likely to reduce harm.

// AREAS FOR IMPROVEMENT

List gaps in authority, plans, contacts, technical controls, continuity, communications or reporting.

// KEY DECISIONS AND UNRESOLVED QUESTIONS

AAR - improvement plan and approval

Track actions until evidence confirms completion

// IMPROVEMENT PLAN

FINDING	ACTION / DELIVERABLE	OWNER	DUE	VALIDATION

Participant feedback summary

Most useful part:

_____

Least clear part:

_____

Additional role/resource needed:

_____

Recommended next scenario:

_____

Approval and follow-up

AAR prepared by: _____

Incident-plan owner: _____

Approved by: _____

Approval date: _____

30-day review: _____

Re-exercise date: _____

Close the loop. Update plans and contact sheets, verify completed controls, report material risks to leadership, and re-exercise the weakest capability rather than repeating the same session unchanged.

Federal and state references

Official government sources only

Source policy:
This pack uses official U.S. federal and state government sources only. URLs and requirements should be checked again before each exercise because guidance and state law may change.

[1] Cybersecurity and Infrastructure Security Agency. CTEP Package Documents - facilitator, planner, feedback and after-action materials. https://www.cisa.gov/resources-tools/resources/ctep-package-documents

[2] Cybersecurity and Infrastructure Security Agency. Cybersecurity Scenarios - CISA Tabletop Exercise Packages addressing ransomware, phishing and other threats. https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios

[3] U.S. Department of Education. K-12 Cybersecurity - emergency operations planning, federal reporting routes and school cyber-resilience resources. https://www.ed.gov/teaching-and-administration/safe-learning-environments/school-safety-and-security/k-12-cybersecurity

[4] Cybersecurity and Infrastructure Security Agency. #StopRansomware Guide - preparation, response, reporting, evidence and recovery guidance. https://www.cisa.gov/stopransomware/ransomware-guide

[5] Federal Bureau of Investigation. Ransomware - reporting to local FBI and IC3; FBI position on ransom payment. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

[6] U.S. Department of Education, Student Privacy Policy Office. Data Security: K-12 and Higher Education. https://studentprivacy.ed.gov/data-security-k-12-and-higher-education

[7] U.S. Department of Education, Student Privacy Policy Office. Password Data Breach Response Training Kit - customizable exercise for education agencies. https://studentprivacy.ed.gov/resources/password-data-breach-response-training-kit

[8] Texas Department of Information Resources. Cybersecurity Incident Management and Reporting - local government and school district reporting. https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting

[9] New York State Division of Homeland Security and Emergency Services. Cybersecurity Incident and Ransom Payment Reporting. https://www.dhses.ny.gov/cybersecurity-incident-and-ransom-payment-reporting

[10] Georgia Emergency Management and Homeland Security Agency. Report a Utility/Agency Cybersecurity Incident. https://gema.georgia.gov/get-involved/report-utilagcy-cybersecurity-incident

[11] California Department of Justice, Office of the Attorney General. Data Security Breach Reporting. https://www.oag.ca.gov/privacy/databreach/reporting

Federal reporting shortcuts. CISA: cisa.gov/report | FBI field offices: fbi.gov/contact-us/field-offices | IC3: ic3.gov

Recommended adoption step. Attach a district-specific state reporting addendum, current contact sheet and restoration-priority list before approving this exercise for annual use.