**Introduction and Facilitator Guide**

These mini tabletop exercises are designed to help K12 schools test their preparedness for various disaster scenarios. Each exercise focuses on different aspects of emergency response and recovery, highlighting the importance of the five critical plans: Crisis Management, Crisis Communication, Cyber Incident & Disaster Response, Educational Continuity, and Technology Recovery.

**How to Use These Exercises**

Each mini tabletop exercise is designed to take approximately 20-30 minutes. Depending on your audience and time constraints, you can:

1. Full Group Discussion: Present the scenario to the entire group and facilitate a discussion using the key points.
2. Small Group Breakouts: Divide participants into small groups, assign each a scenario, and have them work through the key discussion points. Then reconvene for sharing.
3. Role-Based Approach: Assign participants specific roles (Superintendent, Principal, IT Director, etc.) and have them respond from that perspective.
4. Timed Inject Model: Reveal the scenario and then introduce injects at timed intervals, forcing participants to adapt as new information emerges.

**Facilitation Tips**

* Begin each exercise by reading the scenario and giving participants 1-2 minutes to consider initial reactions.
* Use the key discussion points as prompts but allow the conversation to develop naturally.
* Ask participants to identify which of the five critical plans (Crisis Management, Crisis Communication, Cyber Incident & Disaster Response, Educational Continuity, and Technology Recovery) they are drawing from for each decision.
* Connect responses back to the K12 Preparedness Assessment Framework to highlight gaps and strengths.
* Encourage participants to document specific action items for their own schools.
* After each scenario, briefly discuss how the Resilience Roadmap would help them better prepare for similar situations.
* Use the timeline and injects to create a sense of urgency and realism.
* For communications-focused injects, ask participants to draft actual messaging they would use.

**Communication Challenges to Emphasize**

* The tension between speed and accuracy in crisis communications
* Managing social media and addressing rumors with incomplete information
* Communication when normal channels are disrupted
* Balancing transparency with legal/liability concerns
* Coordinating messaging across multiple stakeholders
* Documentation of all communications for after-action review

**Data Management Lessons**

* Highlight the importance of data retention policies and enforcement
* Discuss compliance requirements for different types of student records
* Emphasize the need for documented data handling procedures with vendors
* Illustrate how proper data management reduces breach impact
* Demonstrate the importance of regular data audits and cleanup

**Customization Options**

* Adjust the scenarios to match regional threats (e.g., hurricanes, wildfires, tornadoes)
* Modify system names to match common platforms used in your region
* Add local regulatory requirements specific to your state
* Scale the impacts up or down depending on the size of districts represented
* Customize social media and news injects to reflect platforms popular in your community

Contents

[Exercise 1: Ransomware Attack on Student Information System 3](#_Toc195524881)

[Exercise 2: Severe Weather Event with Extended Power Outage 9](#_Toc195524882)

[Exercise 3: Vendor Platform Data Breach 16](#_Toc195524883)

[Exercise 4: Water Main Break and Building Damage 24](#_Toc195524884)

[Exercise 5: Wildfire Threatening School Facilities 33](#_Toc195524885)

[BONUS CONTENT: Making Mini Tabletop Exercises into Micro Moments 41](#_Toc195524886)

# Exercise 1: Ransomware Attack on Student Information System

Objectives and Success Criteria

1. **Cyber Incident Response Coordination**
   * Objective: Establish and execute an effective incident response to the ransomware attack
   * Success Criteria:
     + Containment actions implemented within 2 hours of discovery
     + Incident response team fully assembled within 4 hours
     + Law enforcement notification completed within 24 hours
     + Clear decision regarding ransom payment made within 48 hours
2. **Crisis Communications Effectiveness**
   * Objective: Communicate timely and accurately with all stakeholders
   * Success Criteria:
     + Initial staff notification completed within 4 hours
     + Parent/guardian notification issued within 8 hours of discovery
     + Media response strategy established within 12 hours
     + Misinformation on social media addressed within 2 hours of appearance
3. **Educational Operations Continuity**
   * Objective: Maintain essential educational functions during system outage
   * SuccessCriteria:
     + Alternate attendance tracking implemented within 24 hours
     + Student medical information recovered through alternative sources
     + No more than 1 day of instruction significantly impacted
     + Essential reporting functions maintained using manual processes
4. **Data Recovery and System Restoration**
   * Objective: Recover critical systems and data with minimal permanent loss
   * SuccessCriteria:
     + Recovery plan with prioritized systems established within 24 hours
     + Critical systems restored within 72 hours
     + Data recovery options fully evaluated within 48 hours
     + System security improvements identified before restoration

Scenario

During a busy Monday morning in October, teachers attempt to take attendance but cannot access the district's Student Information System (SIS). The IT coordinator receives multiple calls and discovers a ransom note on the main administrative computer demanding $175,000 in cryptocurrency. All student records, schedules, contact information, and health data are encrypted and inaccessible.

AttackVector

The ransomware entered through a phishing email sent to the administrative assistant three days earlier. The email appeared to be from the SIS vendor claiming an "urgent security update" was needed. When clicked, it installed malware that harvested credentials and allowed attackers to gain access to the system over the weekend.

Systems Affected

* Student Information System (SIS)
* Attendance tracking
* Student health records
* Parent contact information
* Bus routing information
* Staff email (partially)

Impact to School

* Unable to accurately track student attendance
* Cannot access emergency contact information
* Health alerts for students with medical conditions are unavailable
* Staff cannot email parents
* Bus routes must be run from memory
* Grades and academic records inaccessible
* State-mandated reporting cannot be completed

**Timeline and Injects**

**7:45 AM** - Teachers begin reporting they cannot access the SIS system

* Facilitator Details: The SIS login page appears normal, but after entering credentials, users receive a generic error message. Multiple teachers report this issue separately to both IT and administration.
* *Inject 1:* A diabetic student arrives without his medication information available
  + Facilitator Details: The student requires insulin during the school day. Normally, this information and the insulin dosage are stored in the SIS health module, but now the nurse cannot access it. The student says he "thinks" he needs his medication soon but isn't sure of the dosage. The emergency contact information for his parents is also in the SIS. The student has a medical ID bracelet that confirms his diabetes but doesn't list medication details.
  + Prompt Questions: What immediate actions should be taken to address this medical need? Who has authority to contact emergency services? How can parent contact information be recovered quickly?

**8:30 AM** - IT confirms ransomware attack and notifies principal

* Facilitator Details: The IT coordinator is able to identify this as ransomware because:
  1. When logging into the main administrator computer, a red screen appears with a skull and crossbones image
  2. The text message reads: "All your files have been encrypted. To decrypt your files, you must pay $175,000 in Bitcoin. You have 72 hours to pay or all your data will be permanently deleted and published on the dark web."
  3. When trying to open any file on the server, it shows a .encrypted extension and cannot be opened
  4. The ransom note includes specific instructions for payment and a sample decryption of one small file to prove they control the encryption
  5. The ransomware has also changed desktop wallpapers on connected computers to display the ransom message
* Prompt Questions: Who should be in the initial response team? What immediate containment steps should be taken? What systems should be disconnected or shut down?
* *Decision Point:* Who needs to be notified at this point?
  1. Options to Consider: Superintendent only? Full administrative team? School board? Local law enforcement? FBI? State education department? Insurance provider? Legal counsel?
  2. Discussion Guidance: Focus on the balance between involving necessary stakeholders and maintaining control of information flow

**9:15 AM** - No official communication has been sent to parents yet

* Facilitator Details: Despite awareness of the issue for over an hour, no formal parent notification has been created or distributed. Staff have been told not to discuss the situation with parents or students yet.
* *Inject 2:* A parent posts on Facebook: "My son says the school computers are all broken and they think they got hacked! Anyone know what's going on? #SchoolHacked"
  + Facilitator Details: The post includes a screenshot the student took of a teacher's computer showing an error message when trying to access the SIS. While not the actual ransom note, it clearly shows a system failure.
* *Inject 3:* Post receives 47 shares and 26 comments in 20 minutes, including speculation about student data being stolen
  + Facilitator Details: Comments include inaccurate statements like "My friend works at the district office and says they're demanding a million dollars" and "I heard they have all our kids' Social Security numbers now"
  + Prompt Questions: At what point do social media rumors require an official response? What platforms should be monitored during a crisis? Who is responsible for social media monitoring and response?

**10:00 AM** - Local news station calls the front office asking for comment on the "cyberattack"

* Facilitator Details: The reporter mentions they've received "multiple tips" about a cyberattack and plan to run a story on the noon broadcast. They're asking for confirmation, the extent of the attack, and what parents should know.
* *Decision Point:* What is your immediate response to media?
  + Options to Consider: No comment? Confirmation of "technical issues"? Honest but limited disclosure? Prepared statement? Who is authorized to speak to media?
  + Prompt Questions: What are the legal implications of confirming a data breach before the full scope is known? What information would parents most need at this point?

**11:30 AM** - IT discovers the backup system has been malfunctioning for 3 weeks

* Facilitator Details: The backup system shows successful backup completion in logs, but when IT attempts to restore from backups, they discover the files are corrupted. Further investigation shows the attackers deliberately targeted and compromised the backup system first, then waited before deploying the main ransomware attack.
* *Inject 4:* The last viable backup is from the previous school year, missing all current student data
  + Facilitator Details: The viable backup is from June of the previous school year. It contains basic student information but none of the current year's schedules, grades, health updates, or new student information.
  + Prompt Questions: How does this change the recovery strategy? At what point do you consider paying the ransom? Who makes that decision? What verification systems should be in place to ensure backups are actually working?

**1:00 PM** - Investigation reveals the attack also accessed historical student records

* Facilitator Details: IT discovers that the ransomware also encrypted a server containing archived student records going back many years. These records include more sensitive information than current records, including Social Security Numbers (which were collected prior to a policy change 5 years ago), disciplinary records, and some psychological evaluations.
* *Inject 5:* Records going back 15 years were stored on the same server despite district policy stating records should be archived after 7 years
  + Facilitator Details: The IT team finds documentation showing a data retention policy was approved by the school board 8 years ago requiring deletion of non-essential student records after 7 years. However, the policy was never implemented due to staff turnover and lack of follow-up procedures.
  + PromptQuestions: How does the retention policy violation impact the district's liability? Who is responsible for ensuring compliance with data retention policies? What systems should be in place to automate proper data lifecycle management?
* *Decision Point:* How does this impact your notification requirements?
  + OptionstoConsider: Notify all affected former students? Only notify current students? Different notification for different levels of exposure?
  + DiscussionGuidance: Explore the legal requirements in your state for breach notification when historical records are involved, especially for former students who may be difficult to contact

**3:30 PM** - Parent calls reporting their child received a text message claiming to be from hackers

* FacilitatorDetails: The parent is extremely upset and says their high school student received a text message that included the student's name, address, and date of birth along with a threat. The parent wants to know how the hackers got their child's cell phone number and what the school is doing to protect students.
* *Inject 6:* The message contains personal information and threatens to post student records online if ransom isn't paid
  + FacilitatorDetails: The text reads: "We have all student records from [School Name]. If the school doesn't pay, we will post everything online, including your information: [Student Name], [Address], [DOB]. Tell your parents to pressure the school to pay." The message came from an anonymous texting service and cannot be easily traced.
  + PromptQuestions: How should the district respond to this escalation? What guidance should be given to parents and students about direct contact from attackers? What coordination with law enforcement is needed now?

**Key Discussion Points**

1. Who makes the decision about whether to pay the ransom?
2. How do you track attendance without digital systems?
3. What is your communication plan to parents without access to contact information?
4. How would you handle a medical emergency without access to student health records?
5. What immediate containment steps should IT take?
6. At what point do you involve law enforcement?
7. What is your backup and recovery plan for the SIS?
8. How do you address social media rumors without complete information?
9. What are the legal implications of retaining student records beyond the required retention period?

Facilitator Background Information

**About Ransomware Identification**: Ransomware typically follows predictable patterns that IT staff should be trained to recognize:

* Files suddenly become inaccessible and show unusual extensions (.encrypted, .locked, etc.)
* Ransom notes appear as text files, images, or on-screen wallpapers
* System performance may deteriorate rapidly as encryption processes run
* Unusual network traffic patterns as the ransomware communicates with command-and-control servers
* Antivirus alerts that may identify the specific ransomware variant
* Critical system files or databases become inaccessible with specific error messages

**Regarding School Health Records**:

* Schools are required to have emergency procedures for situations when electronic health records are unavailable
* Paper backup records for students with critical health needs should be maintained
* School nurses typically keep separate notes that may contain some critical information
* HIPAA and FERPA regulations may both apply to student health information

**Law Enforcement Response Expectations**:

* Local police may take initial reports but have limited technical capabilities for cybercrime
* FBI has dedicated cybercrime units but typically only becomes heavily involved in cases with:
  + Critical infrastructure impacts
  + Ransoms exceeding certain thresholds
  + Known criminal groups already under investigation
  + Multiple affected organizations in a coordinated attack
* K12 schools may not receive immediate high-level federal assistance unless the attack is part of a larger pattern

**Data Retention Best Practices**:

* Student records typically have different retention requirements based on type:
  + Permanent records (transcripts): Indefinite retention
  + Health records: Often 1-7 years after graduation
  + Disciplinary records: Often 3-5 years
  + Special education records: Often 5-7 years after services end
* Many districts fail to implement proper retention schedules due to:
  + Lack of technical knowledge to safely delete specific records
  + Concern about deleting something that might be needed later
  + Inadequate documentation of retention requirements
  + No automated process for records management

# Exercise 2: Severe Weather Event with Extended Power Outage

Objectives and Success Criteria

1. **Emergency Response and Student Safety**
   * Objective: Ensure immediate safety of all students and staff during the weather event
   * SuccessCriteria:
     + All students and staff are accounted for within 15 minutes of event
     + No injuries reported due to appropriate shelter procedures
     + Proper emergency protocols followed for building evacuation if necessary
2. **Crisis Communication with Limited Technology**
   * Objective: Establish effective communication with parents, staff, and community without normal channels
   * SuccessCriteria:
     + Initial parent notification completed within 60 minutes of decision to close
     + At least three alternative communication methods identified and utilized
     + Misinformation on social/news media addressed within 2 hours of appearance
3. **Educational Continuity Planning**
   * Objective: Develop and implement plan for continuing education during extended closure
   * SuccessCriteria:
     + Alternative teaching locations secured within 48 hours
     + No more than 3 instructional days lost before resuming in some capacity
     + Clear communication to families about alternative arrangements within 24 hours of securing locations
4. **Resource Coordination and Management**
   * Objective: Effectively coordinate with community partners and emergency services
   * SuccessCriteria:
     + Appropriate emergency management agencies contacted within first hour
     + Resources and mutual aid agreements activated within first day
     + Documentation of all decisions and actions maintained for after-action review

Scenario

A powerful derecho (straight-line windstorm) sweeps through your region with little warning during school hours. The storm causes widespread damage to power infrastructure, including downing multiple power lines on and near school property. Initial estimates from the power company indicate repairs will take 7-10 days. The school building has sustained minor structural damage to the roof over the gymnasium, but the main building is intact. However, with no electricity, heating/cooling systems, network connectivity, and some plumbing systems are inoperable.

Systems Affected

* Electrical infrastructure
* HVAC systems
* Network and internet connectivity
* Phone systems (except emergency backup lines)
* Security systems including electronic door locks
* Water pumps (affecting restroom facilities)
* Refrigeration for food service

Impact to School

* Unsafe to continue normal operations in the building
* No ability to use technology-dependent teaching tools
* Food spoilage in cafeteria
* Limited communication channels with parents and staff
* Safety concerns due to disabled security systems
* Neighboring districts also affected, limiting relocation options

Timeline and Injects

**1:45 PM** - National Weather Service issues severe thunderstorm warning

* Facilitator Details: The warning comes during 7th period. Many students are in elective classes, not their homerooms. Some students are in PE classes outside. The warning estimates severe winds and possible hail within 30 minutes.
* *Decision Point*: Do you dismiss early or shelter in place?
  + Options to Consider:
    - Immediate early dismissal (risking students in transit during storm)
    - Moving to shelter-in-place locations per severe weather plan
    - Holding students until after storm passes, then dismissing early
    - Normal dismissal with modified transportation plans
  + Prompt Questions: How do you account for all students not in regular classrooms? How are parents notified about any change in dismissal? Who makes this decision and what factors should be considered?

**2:10 PM** - Storm hits with extreme winds and heavy rain

* Facilitator Details: Winds reach 70+ mph, well above forecast levels. Flying debris breaks several windows in the north wing. Power flickers several times before going out completely.
* *Inject 1:* Power goes out immediately; backup generator fails to start
  + Facilitator Details: The backup generator is later found to have maintenance issues that weren't addressed. Battery backup emergency lighting works in some areas but not all. Phone lines are still operational but the phone system requires power.
  + Prompt Questions: What immediate actions are taken when power fails? Who is responsible for checking on generator function? What essential systems should have power redundancy?
* *Inject 2:* Cell service becomes spotty as towers are damaged
  + Facilitator Details: Staff report having between 0-1 bars of service. Text messages sometimes get through after multiple attempts but calls frequently drop. Internet-based services like email are completely unavailable.
  + Prompt Questions: What alternative communication methods are available? How do staff communicate within the building without intercoms or phones?

**2:30 PM** - Storm begins to subside

* Facilitator Details: Rain continues but winds decrease. A preliminary assessment shows downed trees in the parking lot and water intrusion in several classrooms from broken windows. The gymnasium roof has visible damage with water dripping onto the floor.
* *Inject 3:* Three students are missing from classroom headcounts
  + Facilitator Details: During the shelter-in-place procedure, three students (all 8th graders) cannot be located. They were last seen heading to the restroom just before the storm hit. The electronic attendance system is down and paper attendance sheets from earlier in the day are in the main office.
  + Prompt Questions: What search procedures should be implemented? Who coordinates the search? How is information about missing students communicated with limited technology?
* *Decision Point:* How do you conduct search with limited communication?
  + Options to Consider:
    - Room-by-room physical search by administrators
    - Using available two-way radios (if any)
    - Establishing a central command point for coordination
    - Deploying staff in teams of two for safety
  + Discussion Guidance: Focus on systematic search procedures that maintain staff safety while ensuring thorough coverage

**3:00 PM** - Parents begin arriving to pick up students despite flooded roads

* Facilitator Details: Despite hazardous conditions, approximately 40-50 parents arrive at the school demanding to pick up their children. Traffic is backing up in the parking lot and on surrounding streets. Some parents parked several blocks away and walked to the school.
* *Inject 4:* Without electronic systems, verifying authorized pickups is challenging
  + Facilitator Details: The emergency contact cards are stored electronically in the SIS with paper backups in the main office. Some teachers have printed class rosters but these don't include approved pickup information. Several parents are demanding to take their children's friends home as well.
  + Prompt Questions: How do you verify authorized pickups without access to records? What alternative identification procedures can be implemented quickly? How do you document who has been picked up?
* *Inject 5:* A local radio station incorrectly reports that the school roof has collapsed
  + Facilitator Details: A news report states: "We're getting reports that Roosevelt Middle School's roof has collapsed from storm damage. No word yet on possible injuries." Parents arriving have heard this report and are frantic for information.
  + Prompt Questions: How do you correct misinformation with limited communication channels? Who is authorized to speak to media during the crisis? How do you reassure panicked parents?

**4:15 PM** - Emergency management officials arrive

* Facilitator Details: County emergency management and fire department personnel arrive to assess the building. They do a walkthrough with the principal and facilities manager.
* *Inject 6:* They advise the building should not be occupied until structural assessment is complete
  + Facilitator Details: Officials determine that while there's no imminent danger, the building should not be occupied for regular instruction until a structural engineer can assess the gymnasium roof damage and electrical systems can be inspected after power is restored. Their estimate is at least 3-5 days before this assessment can be completed.
  + Prompt Questions: How does this impact your immediate vs. long-term planning? What communication needs to occur with district leadership? When and how do you notify staff about work expectations?
* *Decision Point:* How do you determine where to hold classes tomorrow?
  + Options to Consider:
    - Distance learning (if feasible with technology limitations)
    - Canceling school for several days
    - Seeking emergency space in community facilities
    - Modified schedules at other district schools
  + Discussion Guidance: Examine criteria for evaluating alternative locations, including transportation logistics, facility requirements, and safety considerations

**6:00 PM** - Most students have been picked up

* Facilitator Details: Approximately 85% of students have been picked up. Documentation of pickups has been managed through an improvised paper system. The remaining students include those whose parents work evening shifts, lack transportation, or haven't been reached.
* *Inject 7:* Ten students remain whose parents haven't been reached
  + Facilitator Details: Multiple attempts to contact these parents have failed. Cell service remains unreliable, and some families live in areas more severely affected by the storm. The remaining students include two with medical needs (asthma and ADHD) whose medications are typically dispensed at the end of the school day.
  + Prompt Questions: What protocols exist for students who cannot be picked up? Who is authorized to stay with students after hours? How are medical needs addressed without access to regular health records?
* *Inject 8:* Social media fills with parents complaining about lack of communication
  + Facilitator Details: Posts on community Facebook groups and Twitter include: "School hasn't sent ANY updates about the storm damage!" and "Why weren't kids sent home BEFORE the storm hit?" Several influential parents are demanding answers from district leadership.
  + Prompt Questions: How do you address parent concerns without reliable communication channels? What proactive steps could have prevented this situation? How do you document the decision-making process for potential criticism later?

**Day 2, 8:00 AM**

* Facilitator Details: Overnight assessment confirms widespread power outages affecting approximately 60% of the district. Three main transmission lines were damaged, supporting the power company's 7-10 day restoration estimate. Cell service has improved somewhat but remains unreliable.
* *Inject 9:* The superintendent has been unable to reach several school board members
  + Facilitator Details: Key decisions about extended closure and alternative locations require board notification or approval per district policy. Several board members live in areas with no cell service, and the board president is traveling out of state.
  + Prompt Questions: What contingency plans exist for governance during emergencies? What decisions can be made without board approval? How is emergency decision-making authority documented?
* *Inject 10:* Local church offers space, but requires religious symbols remain in place
  + Facilitator Details: A large church three miles from the school offers their education wing (8 classrooms) at no cost. However, the rooms contain religious artwork and symbols that they are unwilling to remove. The church can accommodate the space for up to two weeks.
  + Prompt Questions: What legal or policy considerations exist for using religious facilities? How would you address concerns from diverse families? What alternatives exist if this space is declined?
* *Decision Point:* What is your continuity plan for the next 7-10 days?
  + Options to Consider:
    - Full cancellation until building is reopened
    - Hybrid model using available community spaces
    - Split schedule with morning/afternoon sessions
    - Temporary distance learning with packet pickup
  + Discussion Guidance: Consider how any plan impacts different student populations, especially those with limited resources or special needs

**Day 3, 10:00 AM**

* Facilitator Details: The district has established a command center at the central office using generator power. Communication has improved with the acquisition of satellite phones for key personnel. A structural engineer has confirmed the gymnasium needs extensive repairs but the rest of the building could potentially be occupied once power is restored and safety systems are functional.
* *Inject 11:* Health department expresses concerns about food storage and preparation at temporary locations
  + Facilitator Details: Any plan to serve meals at alternative locations must meet health department requirements for food safety. The normal kitchen equipment cannot be moved, and refrigerated items at the school have spoiled due to power loss.
  + Prompt Questions: How do you maintain food service for students who depend on school meals? What agreements exist with vendors for emergency meal provision? Are there funding implications for modified meal service?
* *Inject 12:* It's discovered that emergency contact information printed at the beginning of the year is stored at the school and inaccessible
  + Facilitator Details: The emergency preparedness plan called for printed emergency contacts to be stored in multiple locations, but all copies are in the administrative office at the school. No off-site backup exists.
  + Prompt Questions: How do you rebuild critical contact information? What redundancies should exist for emergency information? Who is responsible for ensuring emergency protocols are followed?

**Key Discussion Points**

1. What is your immediate response when the storm hits?
2. How do you account for all students and staff during and after the event?
3. What alternative locations could be used for continuing education?
4. What non-technology dependent teaching resources are available?
5. How do you communicate with parents without normal channels?
6. What partnerships exist with community organizations that could provide temporary space?
7. What criteria would you use to determine when to reopen?
8. How would you coordinate with emergency management authorities?
9. How do you address public misinformation during an ongoing crisis?
10. What emergency supplies should be stored offsite or in multiple locations?

Facilitator Background Information

**About Derecho Weather Events**:

* Derechos are widespread, long-lived windstorms associated with rapidly moving showers or thunderstorms
* They can produce damage similar to tornadoes but typically in one direction along a relatively straight path
* Advance warning may be limited compared to hurricanes or winter storms
* They typically occur during warm weather months but can happen any time of year
* Weather alerts may initially be issued as severe thunderstorm warnings rather than specifically identifying a derecho

**Power Outage Impacts on School Systems**:

* Modern schools have numerous systems that fail without power:
  + Electronic door access controls may default to locked or unlocked positions
  + Sewage ejector pumps may stop functioning in buildings without gravity systems
  + Phone systems, even landlines, often require power for distribution to classrooms
  + Public address/intercom systems for emergency communication
  + Refrigeration for food service, science materials, and medications
  + Computer networks, servers, and wireless access points

**Alternative Facility Requirements**:

* Any alternative teaching space must address:
  + ADA accessibility requirements
  + Minimum square footage per student requirements (varies by state)
  + Basic safety standards and emergency exits
  + Restroom facilities appropriate for student age groups
  + Food service or dining areas if providing meals
  + Appropriate supervision ratios based on space configuration

**Legal Considerations for Religious Facilities**:

* Schools may use religious facilities as emergency locations if:
  + The arrangement is clearly temporary
  + No religious instruction occurs
  + Attendance is not used for religious recruitment
  + The space is offered on the same terms as it would be to other community organizations
* Courts have generally allowed such arrangements in emergency circumstances provided neutrality is maintained

# Exercise 3: Vendor Platform Data Breach

Objectives and Success Criteria

1. **Breach Response Management**
   * Objective: Establish and implement an effective vendor-related incident response process
   * Success Criteria:
     + Initial assessment of breach impact completed within 4 hours of notification
     + Proper escalation to appropriate leadership within 1 hour of confirmation
     + Documentation of all vendor communications maintained throughout incident
2. **Stakeholder Communication**
   * Objective: Provide timely and appropriate notifications to all affected stakeholders
   * Success Criteria:
     + Initial staff notification issued within 4 hours of confirmation
     + Parent/guardian communication distributed within 24 hours
     + Regulatory agencies notified within legal timeframes (varies by state)
     + All communications coordinated through single source to ensure consistency
3. **Educational Continuity**
   * Objective: Maintain essential educational functions during system outage
   * Success Criteria:
     + Alternative assessment and content delivery methods identified within 48 hours
     + No more than 1 day of instructional time lost due to system unavailability
     + Teachers provided with clear guidelines for alternative procedures within 24 hours
4. **Data Protection and Legal Compliance**
   * Objective: Address data protection requirements and legal obligations
   * Success Criteria:
     + All potentially affected data identified and documented within 48 hours
     + Compliance with state and federal breach notification laws
     + Appropriate evidence preservation procedures implemented within 24 hours
5. **Vendor Management Improvement**
   * Objective: Strengthen vendor management practices to prevent future incidents
   * Success Criteria:
     + Vendor contract and SLA review completed within 2 weeks
     + Data retention audit conducted for all vendor systems within 30 days
     + Improved vendor security assessment procedures documented and implemented

Scenario

Your district receives an urgent notification from your learning management system (LMS) vendor that they have experienced a significant data breach. The vendor confirms that unauthorized access occurred over the past three weeks, potentially exposing student and teacher account information, grades, assignments, and some assessment data. The vendor has temporarily taken their system offline for investigation and remediation, with an estimated restoration timeline of 1-2 weeks.

**Attack Vector**

The breach originated through a compromised administrator account at the vendor. The attack was sophisticated and appears to be targeted specifically at educational institutions. Early investigation suggests the attackers were primarily interested in gathering personal information rather than disrupting services.

**Systems Affected**

* Learning Management System
* Online assessment platform
* Teacher gradebooks
* Student assignment submissions
* Parent portal access
* Integration with other educational tools

**Impact to School**

* Teachers cannot access lesson plans or instructional materials
* Students cannot access assignments or submit work
* Online assessment platform unavailable during scheduled testing period
* Potential exposure of student Personal Identifiable Information (PII)
* Possible regulatory implications under state student privacy laws
* Parent and community concern about data security

Timeline and Injects

**Day 1 - 9:15 AM** - Vendor sends email notification of breach to district IT director

* Facilitator Details: The email is somewhat vague, stating only that they are "investigating a security incident" and have taken systems offline as a precaution. The email mentions "potential unauthorized access" but provides no specifics about what data may have been compromised. The email indicates more information will be forthcoming.
* *Inject 1:* IT director is out sick and hasn't seen the notification
  + Facilitator Details: The IT director is home with the flu and has not checked email since the previous evening. There is no automated forwarding or out-of-office notification set up. The email was sent only to the IT director's address, not to a department alias that others might monitor.
  + Prompt Questions: What backup notification procedures should be in place for critical communications? How should vendor contact information be managed to ensure redundancy? Who should be designated as backup points of contact?
* Discussion Guidance: Focus on the implications of single points of failure in critical communication channels and the importance of role-based rather than individual-based contact information

**Day 1 - 11:30 AM** - Teachers begin reporting LMS access issues

* Facilitator Details: Multiple teachers report error messages when trying to access the LMS. The system displays a generic "System Temporarily Unavailable" message with no additional information. Teachers have assignments due today and need to access student submissions.
* *Inject 2:* A teacher posts in a private Facebook group: "LMS is down again. Anyone know what's happening?"
  + Facilitator Details: The post is in a closed group with about 75 district teachers as members. Several respond that they're also having issues, and speculation begins about whether the district forgot to pay the bill or if there's a technical problem.
  + Prompt Questions: How do you manage unofficial communication channels during an incident? What responsibilities do staff have regarding discussion of school issues on social media? How do you ensure staff receive accurate information quickly?
* *Inject 3:* Several teachers reply they heard it was "hacked"
  + Facilitator Details: One teacher comments that her friend at another district said their LMS was also down and they were told it was "some kind of hack." This information spreads quickly among the group, with teachers beginning to worry about their personal information and gradebooks.
  + Prompt Questions: At what point should administration address rumors among staff? What initial information can be shared before full details are known? Who should communicate with staff about technology issues?

**Day 1 - 1:45 PM** - Principal learns about the situation

* Facilitator Details: The principal learns about the outage from teachers, not through official channels. Upon investigation, an assistant in the IT office finds the email and forwards it to the principal and superintendent. This is the first official notification school leadership has received.
* *Decision Point*: Do you communicate with parents now or wait for complete information?
  + Options to Consider:
    - Immediate notification that system is down with minimal details
    - Wait for more complete information from vendor
    - Limited notification to only those with imminent needs (e.g., testing)
    - Different messages to staff vs. parents
  + Discussion Guidance: Explore the tension between speed and accuracy in crisis communications, and the risks of both premature and delayed communication
* *Inject 4:* State testing window opens in three days
  + Facilitator Details: The district is scheduled to begin standardized testing that requires the LMS platform for delivery. Rescheduling is possible but complicated and would require state department of education approval.
  + Prompt Questions: What contingency plans should exist for testing when primary systems fail? What stakeholders need to be involved in decisions about testing modifications? What documentation is required for state reporting if testing is delayed?

**Day 1 - 3:20 PM** - Still no official communication to parents

* Facilitator Details: The leadership team has been gathering information but has not yet sent any communication to parents. Students have been telling parents they couldn't submit assignments or access materials, leading to confusion.
* *Inject 5:* A parent calls the local news station about "a data breach affecting children's private information"
  + Facilitator Details: The parent is a privacy advocate who has previously expressed concerns about educational technology. They have limited accurate information but are concerned about potential exposure of student data.
  + Prompt Questions: How do you respond to media inquiries with limited verified information? What privacy laws might apply to this situation? Who serves as media spokesperson in a technology-related incident?
* *Inject 6:* News station posts on their website: "BREAKING: School District Data Hack Exposes Student Information"
  + Facilitator Details: The article contains multiple inaccuracies, including that the district's "computer system was hacked," that "hackers stole student Social Security Numbers" (which weren't in the system), and that the district "has refused to comment on the situation."
  + Prompt Questions: What is your strategy for correcting public misinformation? How do you balance transparency with the need for accurate information? What legal implications exist for confirming specific details about a data breach?

**Day 2 - 8:00 AM** - Superintendent contacts vendor for clarification

* Facilitator Details: After limited updates from the vendor, the superintendent directly calls the vendor's executive team demanding more information. The vendor agrees to a conference call with district leadership.
* *Inject 7:* Vendor admits they're unsure exactly what data was accessed
  + Facilitator Details: The vendor reports that logs show unauthorized access to their database servers, but they cannot yet determine which specific records or data elements were viewed or extracted. Their investigation is ongoing with third-party forensic assistance.
  + Prompt Questions: How does uncertainty about affected data impact your notification strategy? What assumptions should you make about data exposure when specific details are unknown? What remediation steps can be taken even without complete information?
* *Inject 8:* Vendor reveals breach may have affected archived data going back 5+ years
  + Facilitator Details: The compromised servers contained not just current student data but historical data going back to when the system was first implemented. This potentially includes information on students who have graduated or left the district.
  + Prompt Questions: What obligations do you have to former students and staff? How do you locate and notify people who are no longer affiliated with the district? What data retention limitations should be included in vendor contracts?

**Day 2 - 10:30 AM** - District sends first communication to parents

* Facilitator Details: The district sends an email and text alert to all parents explaining the vendor system is down due to a "security incident" and providing basic information about alternative assignment submission methods and the potential for rescheduled testing.
* *Inject 9:* IT discovers the district never deleted historical student data from vendor platform despite students leaving the district
  + Facilitator Details: During an emergency audit of what data the vendor maintains, IT realizes that the district has never implemented a data deletion process for students who graduate or transfer. All historical accounts remain active but dormant in the system.
  + Prompt Questions: What data retention and deletion procedures should be standard practice? Who is responsible for ensuring data minimization principles are followed? What automation could prevent this type of oversight?
* *Inject 10:* District's contract with vendor doesn't clearly specify data retention responsibilities
  + Facilitator Details: Legal review of the vendor contract reveals vague language about data management responsibilities. The contract states the vendor will maintain data "in accordance with district policies" but doesn't specify those policies or establish clear retention limits.
  + PromptQuestions: What specific terms should be included in vendor contracts regarding data retention and deletion? How often should contracts be reviewed for privacy and security provisions? Who should review technology contracts before signing?

**Day 2 - 2:00 PM** - Parent forum organized to address concerns

* FacilitatorDetails: The superintendent schedules an evening virtual meeting for parents to address concerns. Approximately 200 parents plan to attend based on registration.
* *Inject 11:* Parents demand to know exactly what personal information was exposed
  + FacilitatorDetails: During the forum, multiple parents ask specifically what data elements were compromised and whether their children's information is now "on the dark web." They're asking for specifics that the district doesn't yet have.
  + PromptQuestions: How do you address parent concerns when information is incomplete? What resources can you provide to concerned parents about identity protection? How do you maintain trust while acknowledging uncertainty?
* *Inject 12:* A privacy advocacy group contacts the district about a potential lawsuit
  + FacilitatorDetails: A national digital privacy organization emails the superintendent suggesting the district may have violated state student privacy laws by not ensuring proper data protection and retention practices with vendors.
  + PromptQuestions: What documentation should be maintained regarding the district's vendor management practices? What legal counsel should be consulted during a data breach? How do you balance transparency with legal risk management?

**Day 3 - 9:00 AM** - State Department of Education requests explanation

* FacilitatorDetails: The state education agency's data security office contacts the district requesting a full briefing on the incident, including what specific data was exposed, remediation steps, and potential impacts on state reporting and testing requirements.
* *Inject 13:* Initial investigation indicates Social Security Numbers were stored in an optional form field for some students
  + FacilitatorDetails: While the LMS doesn't have a designated field for SSNs, the vendor discovers that an optional "Other ID" field was sometimes used by staff to store SSNs for certain scholarship and program applications, affecting approximately 120 students.
  + PromptQuestions: What policies should exist regarding storage of sensitive information in vendor systems? How do you train staff on appropriate data handling procedures? What audit processes would identify this type of misuse before an incident?
* *Decision Point:* What identity protection services, if any, should be offered?
  + Options to Consider:
    - Credit monitoring for affected students only
    - Credit monitoring for all students as a precaution
    - Information-only resources without paid services
    - Different approaches based on data sensitivity
  + Discussion Guidance: Discuss the costs vs. benefits of identity protection services, legal implications of offering or not offering services, and practical considerations for implementation

**Key Discussion Points**

1. Who is responsible for communicating with different stakeholder groups?
2. What is your message to parents concerned about their children's data?
3. How can teachers continue instruction without access to the LMS?
4. What regulatory notification requirements apply in your state?
5. How do you assess the vendor's security practices moving forward?
6. What alternative assessment methods can be implemented immediately?
7. What documentation should be maintained for potential legal issues?
8. How can you verify what specific data was compromised?
9. What data retention policies should be in place for vendor systems?
10. How do you manage media relationships during an evolving crisis with incomplete information?

Facilitator Background Information

**Understanding Education Data Breaches**:

* Education sector breaches typically involve:
  + Larger scope than initially reported (historically 30-60% larger)
  + Longer detection times than average (often 180+ days)
  + Mixed data types of varying sensitivity
  + Multiple affected groups (current students, former students, staff)
* LMS systems commonly contain:
  + Student directory information (name, grade, email, etc.)
  + Academic performance data (grades, assessments, comments)
  + Behavioral observations in teacher feedback
  + Accommodations information that may indicate disabilities
  + Parent/guardian contact information
  + Rarely: highly sensitive data like SSNs, financial information, detailed medical information (though misuse of fields happens)

**Regulatory Considerations**:

* Federal laws with potential implications:
  + FERPA (Family Educational Rights and Privacy Act)
  + COPPA (Children's Online Privacy Protection Act) for students under 13
  + PPRA (Protection of Pupil Rights Amendment)
* State laws vary significantly but many include:
  + Specific breach notification timelines (typically 30-60 days)
  + Requirements for notification content
  + Potential penalties for delayed notification
  + Requirements for preventative security measures

**Vendor Management Best Practices**:

* Standard contractual elements should include:
  + Clear data ownership statements (district owns all data)
  + Specific retention and deletion requirements
  + Security standards and compliance requirements
  + Breach notification obligations (typically 24-48 hours)
  + Data transfer and return procedures upon contract termination
  + Prohibition on using student data for marketing or product development
  + Regular security assessment requirements
  + Limitations on subcontractor access

**Alternative Instruction Methods**:

* Low-tech alternatives to LMS platforms include:
  + Paper packet distribution for assignments
  + Temporary email submission of assignments
  + Shared network drives (if available and separate from affected systems)
  + Alternative assessment approaches (project-based vs. online testing)

# Exercise 4: Water Main Break and Building Damage

Objectives and Success Criteria

1. **Emergency Response and Damage Mitigation**
   * Objective: Implement immediate response to minimize building and equipment damage
   * SuccessCriteria:
     + Water flow stopped within 30 minutes of discovery
     + Critical equipment and records protected or removed within 2 hours
     + Professional restoration services engaged within 4 hours
     + Proper documentation of damage initiated within first hour
2. **Rapid Communication and Notification**
   * Objective: Effectively notify all stakeholders of closure and alternative plans
   * SuccessCriteria:
     + Initial closure notification distributed to all families within 2 hours
     + Staff notification completed with 100% confirmation of receipt
     + Partner organizations and contractors notified of situation within 4 hours
     + Regular updates provided at least daily throughout closure period
3. **Technology Recovery and Data Restoration**
   * Objective: Recover critical technology systems and data to support operations
   * SuccessCriteria:
     + Salvageable equipment identified and secured within 24 hours
     + Critical data services restored via alternative means within 48 hours
     + Comprehensive technology recovery plan developed within 3 days
     + Complete documentation of lost/damaged equipment for insurance purposes
4. **Educational Continuity Implementation**
   * Objective: Maintain educational services with minimal disruption to students
   * SuccessCriteria:
     + Alternative locations secured within 48 hours
     + No more than 3 instructional days lost before resuming in some capacity
     + Transportation plan for alternative locations developed within 72 hours
     + Special education services maintained in compliance with IEP requirements
5. **Long-term Recovery Planning**
   * Objective: Develop and implement comprehensive recovery and restoration plan
   * SuccessCriteria:
     + Complete damage assessment document created within 1 week
     + Insurance claims properly filed with all required documentation
     + Restoration timeline established with clear milestones and responsibilities
     + Prevention measures identified to mitigate future similar incidents

Scenario

At 4:30 AM on a Tuesday in February, the facilities manager discovers a major water main break inside the school. The break has caused significant flooding throughout the first floor, including the main office, several classrooms, the library, and the server room. Initial assessment indicates 3-4 inches of standing water in affected areas, damaged infrastructure, and no electricity in parts of the building due to safety cutoffs. The environmental control systems in the server room failed, and several physical servers are water-damaged.

**Systems Affected**

* Physical building infrastructure
* Main administrative office
* Library and media center
* Several first-floor classrooms
* On-premises servers including:
  + Local file storage
  + Print servers
  + Building management systems
  + Security camera archive

**Impact to School**

* Building unusable for at least 2-3 weeks during cleanup and repairs
* Significant loss of teaching materials and resources
* Water damage to physical records and documents
* Loss of locally stored data and applications not backed up to cloud
* Disruption to all normal school operations
* Potential mold and air quality concerns

**Timeline and Injects**

**4:30 AM** - Facilities manager discovers water main break

* FacilitatorDetails: The facilities manager arrived early to prepare for a scheduled HVAC maintenance and found water pouring from the ceiling in the main hallway. The break is in an overhead pipe running above the main office area. Water has spread to multiple areas on the first floor, with the heaviest concentration in the administrative area and adjacent server room.
* *Inject 1:* Water has already been flowing for approximately 3 hours
  + FacilitatorDetails: Based on the water volume and security camera timestamps (which stopped recording when the server room was affected), the break likely occurred around 1:30 AM. An estimated 500-1,000 gallons of water have affected the building.
  + PromptQuestions: What emergency shutoff procedures should staff know? How frequently should buildings be checked during off-hours? What water detection systems might have provided earlier warning?
* *Decision Point:* Who needs to be notified immediately?
  + OptionstoConsider:
    - Facilities team only for initial assessment
    - Principal and key administrators
    - Full leadership team including superintendent
    - School board chair
    - Insurance company representative
  + DiscussionGuidance: Focus on the immediate notification chain and the information needed by each party. Consider time of day in determining appropriate notifications.

**5:15 AM** - Superintendent and principals arrive on scene

* Facilitator Details: District leadership arrives to assess the situation. The water main has been shut off, but standing water remains throughout the affected areas. Ceiling tiles have collapsed in several areas, and electrical systems in those zones have been shut down as a precaution.
* *Inject 2:* Insurance representative cannot arrive until tomorrow
  + Facilitator Details: The district's insurance representative is currently at another emergency situation and cannot arrive on site for at least 24 hours. They request immediate documentation of the damage via photos and video before cleanup begins.
  + Prompt Questions: What documentation procedures should be in place for insurance purposes? Who is responsible for this documentation? What information is most critical to capture before remediation begins?
* *Inject 3:* IT director reports server room heavily affected with equipment underwater
  + Facilitator Details: The server room has approximately 2-3 inches of standing water. Several rack-mounted servers on lower shelves were partially submerged. The uninterruptible power supply (UPS) automatically shut down when water was detected, but not before several systems were exposed to water while powered.
  + Prompt Questions: What immediate steps should be taken with water-damaged technology? What recovery priorities should be established for IT systems? What alternative systems can be activated while primary systems are down?

**6:00 AM** - Decision made to cancel school for the day

* Facilitator Details: After assessing the extent of damage, the superintendent decides to cancel classes for the day. Initial estimates suggest at least several days will be needed before any portion of the building is usable.
* *Inject 4:* Emergency notification system malfunctioning due to server damage
  + Facilitator Details: The district's automated notification system for closures runs on one of the affected servers. The system cannot be accessed to send alerts about the school closure.
  + Prompt Questions: What backup communication methods should be established for emergencies? Who has authority to enact these alternative methods? How is contact information maintained in multiple locations?
* *Inject 5:* Local radio station needs information for morning broadcast in 15 minutes
  + Facilitator Details: The local radio station calls the superintendent's cell phone requesting information about the closure for their 6:15 AM broadcast, which many parents rely on for closure information.
  + Prompt Questions: What essential information should be included in initial closure announcements? Who is authorized to provide this information? How do you ensure consistency across different communication channels?
* *Decision Point:* How do you notify all families quickly?
  + Options to Consider:
    - Local media (TV, radio) announcements only
    - Phone tree activation through staff and PTA
    - Social media announcements
    - Website updates (if accessible remotely)
    - Direct staff calling of families
  + Discussion Guidance: Explore the effectiveness and limitations of each communication method, especially considering timing and family access to different communication channels

**7:30 AM** - Despite cancellation notice, some buses and students arrive

* Facilitator Details: Despite efforts to communicate the closure, approximately 30 students arrive via 3 buses, and about 15 parent vehicles drop off students. Some families did not receive any notification about the closure.
* *Inject 6:* A parent posts photos of water flowing from building on social media
  + Facilitator Details: A parent who came to drop off their child takes photos of the water damage visible from outside (including restoration company vehicles and water being pumped out) and posts them on Facebook with the caption: "Massive flood at school today! Looks really bad - hope they can fix it soon!"
  + Prompt Questions: How do you manage unofficial communications about the incident? What information should be provided to counter potential misinformation? Who monitors social media during a crisis?
* *Inject 7:* Physical student records in guidance office are water-damaged
  + Facilitator Details: Staff discover that the bottom drawers of file cabinets in the guidance office containing student records are waterlogged. These include some paper copies of individualized education plans (IEPs), psychological evaluations, and historical records not fully digitized.
  + Prompt Questions: What record recovery procedures should be initiated? What privacy concerns exist for damaged confidential records? What regulatory notifications are required for damaged educational records?

**10:00 AM** - Emergency response team meeting

* Facilitator Details: District leadership convenes to develop initial response plans. Water remediation crews are on site beginning water extraction and dehumidification. Initial damage assessment continues.
* *Inject 8:* Initial assessment shows paper personnel records from 1985-2010 were stored in cardboard boxes on office floor
  + Facilitator Details: Human resources documents including past employee evaluations, employment contracts, and disciplinary actions were stored in non-waterproof containers on the floor of a storage room. Most are heavily water damaged with some text becoming illegible.
  + Prompt Questions: What record retention requirements apply to personnel files? What documentation should be created regarding the lost records? What record storage improvements should be implemented in the future?
* *Inject 9:* It's discovered no inventory of technology equipment exists for insurance purposes
  + Facilitator Details: When asked by insurance to provide a detailed list of damaged equipment with purchase dates and values, IT staff realize no comprehensive inventory has been maintained. Serial numbers and purchase information will need to be reconstructed from purchase orders and partial records.
  + Prompt Questions: What asset management procedures should be standard practice? How frequently should technology inventories be updated? Who is responsible for maintaining this information?
* *Decision Point:* What immediate documentation is needed?
  + Options to Consider:
    - Photos/video only before moving anything
    - Detailed written inventory of visible damage
    - Serial number collection from damaged equipment
    - Statements from staff about items in their rooms
  + Discussion Guidance: Focus on balancing the need for thorough documentation with the urgency of water removal and damage mitigation

**2:00 PM** - Media requests interviews about extent of damage

* FacilitatorDetails: Local television and newspaper reporters arrive at the school requesting information about the incident, how it will affect students, and how long repairs might take.
* *Inject 10:* Restoration company estimates minimum 3-week closure
  + FacilitatorDetails: After more thorough assessment, the water damage restoration company indicates that proper structural drying will take at least 7-10 days, followed by reconstruction of damaged areas. They recommend no occupancy during this time due to ongoing dehumidification needs and air quality concerns.
  + PromptQuestions: What factors should be considered in communicating recovery timelines to the public? How specific should early estimates be? Who should be involved in determining official timelines?
* *Inject 11:* Parents demanding answers about continuity of education
  + FacilitatorDetails: The district office begins receiving numerous calls and emails from parents concerned about educational impacts, particularly from parents of students with special needs and those preparing for important exams.
  + PromptQuestions: What information can be provided to parents within the first 24 hours? How do you address the needs of students with IEPs during alternative arrangements? What special considerations exist for certain student populations?

**Day 2 - 8:00 AM** - Planning for alternative locations begins

* FacilitatorDetails: District leadership begins contacting potential alternative facilities to temporarily house students during repairs. Various options present different advantages and challenges.
* *Inject 12*: Local community college offers classroom space from 4-9 PM only
  + FacilitatorDetails: A nearby community college can provide 15 classrooms but only during evening hours after their own classes end at 4:00 PM. The spaces are well-equipped but would require significant schedule adjustments.
  + PromptQuestions: What factors should be considered in evaluating alternative schedules? How would transportation, food service, and extracurricular activities be affected? What stakeholder input should be gathered before making scheduling changes?
* *Inject 13*: Elementary school in neighboring district offers 6 classrooms during regular hours
  + FacilitatorDetails: A nearby elementary school has a recently closed wing that could accommodate some students during normal school hours. However, the space would only handle about 30% of the student population and would require transportation across district lines.
  + PromptQuestions: What criteria should guide decisions about splitting student populations? What administrative challenges arise from operating in another district's facilities? How do you maintain school cohesion when physically separated?
* *Decision Point*: How do you allocate space and prioritize which grades/classes continue?
  + Options to Consider:
    - Priority to graduating students/testing grades
    - Rotating schedule with different grades on different days
    - Remote learning for some grades, in-person for others
    - Special education and highest-need students prioritized
  + Discussion Guidance: Explore the educational, logistical, and equity implications of different prioritization approaches

**Day 3 - 1:00 PM** - IT assessment completed

* Facilitator Details: After thorough examination, the IT team provides a comprehensive report on technology impacts. They've been working to establish temporary systems using cloud resources and recovered equipment.
* *Inject 14*: 60% of locally stored data is unrecoverable
  + Facilitator Details: Despite recovery efforts, a significant portion of data on the water-damaged servers cannot be recovered. This includes teacher shared drives, some historical student records, and local application data.
  + Prompt Questions: What data recovery services should be considered? How should lost data be documented? What changes to data storage architecture would prevent similar losses in the future?
* *Inject 15*: It's discovered the last cloud backup was 8 months ago due to lapsed subscription
  + Facilitator Details: The automated cloud backup system subscription expired 8 months ago due to a missed renewal notice. The system appeared to be functioning in dashboard views, but no actual backups were being created or stored.
  + Prompt Questions: What oversight systems should exist for critical IT services? Who should receive renewal notifications for essential services? What auditing procedures would have identified this issue proactively?
* *Decision Point*: How do you recreate lost records and materials?
  + Options to Consider:
    - Request copies from staff home computers (for teaching materials)
    - Recreate from state reporting system snapshots
    - Request data from other integrated systems
    - Accept the loss and rebuild from scratch
  + Discussion Guidance: Discuss the practical and legal implications of different approaches to data recovery and recreation

**Day 5 - 10:00 AM** - State Department of Education contacts superintendent

* Facilitator Details: State education officials reach out regarding instructional requirements and reporting obligations given the extended closure.
* *Inject 16*: Questions arise about meeting required instructional hours for the year
  + Facilitator Details: State regulations require a minimum number of instructional hours per school year. The extended closure, combined with previous snow days, puts the district at risk of falling below this threshold.
  + Prompt Questions: What options exist for making up instructional time? What state waiver processes might apply in disaster circumstances? How should instructional hour calculations be documented during alternative arrangements?
* *Inject 17*: Some parents threatening to transfer students to other districts
  + Facilitator Details: A small but vocal group of parents express frustration with the situation and indicate they're considering transferring their children to neighboring districts or private schools if a satisfactory plan isn't implemented quickly.
  + Prompt Questions: How do you address parent concerns about educational continuity? What retention strategies should be considered? How might transfers impact district funding and staffing?

**Key Discussion Points**

1. What immediate steps would be taken to secure and salvage technology equipment?
2. How would you implement your educational continuity plan?
3. What alternative locations could host displaced classes?
4. What communication plan would you activate for staff, students, and parents?
5. How would you prioritize technology recovery efforts?
6. What documentation is needed for insurance claims?
7. How would you manage split operations if only part of the building remains usable?
8. What mutual aid agreements exist with neighboring districts?
9. How would transportation be adjusted for alternative locations?
10. What data retention policies should be established after recovery?
11. How do you maintain regular communication with parents during an extended closure?
12. What is the decision-making process for determining if/when to use outdoor or unconventional teaching spaces?

Facilitator Background Information

**Water Damage Recovery Best Practices**:

* Critical timeline considerations:
  + Mold can begin growing within 24-48 hours
  + Electronic equipment has better recovery chances if dried before corrosion begins
  + Document recovery is most successful when initiated immediately
  + Structural damage assessment should precede any reoccupation
* Professional water restoration typically includes:
  + Water extraction and removal
  + Structural drying with industrial dehumidifiers
  + Mold prevention treatment
  + Air quality testing before reoccupancy
  + Reconstruction of damaged materials

**Technology Recovery Priorities**:

* Standard priority sequence for school technology recovery:
  1. Communication systems (phone, email)
  2. Student information systems for attendance and essential records
  3. Financial/payroll systems
  4. Instructional technology
  5. Administrative systems
  6. Archival and non-essential systems
* Data recovery options include:
  1. Professional data recovery services (expensive but often effective)
  2. Disaster recovery from backup systems (if available)
  3. Partial recovery from integrated systems that contain duplicated data
  4. Reconstruction from physical records where available

**Insurance Considerations for Schools**:

* Most school insurance policies have specific requirements for:
  + Initial documentation before cleanup (photos, videos, inventory)
  + Mitigation efforts to prevent further damage
  + Vendor selection for restoration services
  + Replacement vs. repair determinations
  + Business interruption coverage limitations
  + Technology replacement (actual value vs. replacement cost)
* Common insurance pitfalls include:
  + Inadequate documentation of damaged items
  + Failure to mitigate ongoing damage
  + Missing coverage for specific types of property
  + Inadequate business interruption coverage
  + Exclusions for certain types of water damage

**Alternative Facility Requirements**:

* Any alternative facility must address:
  + Safety standards including fire protection and emergency exits
  + ADA accessibility compliance
  + Appropriate restroom facilities
  + Food service capabilities or alternatives
  + Transportation logistics
  + Communication infrastructure
  + Appropriate supervision spaces

# Exercise 5: Wildfire Threatening School Facilities

Objectives and Success Criteria

1. **Emergency Evacuation and Student Safety**
   * Objective: Ensure safe and orderly evacuation of all students and staff
   * SuccessCriteria:
     + All students and staff accounted for within 15 minutes of evacuation order
     + 100% accurate accounting of all individuals on campus
     + Evacuation completed in accordance with emergency procedures
     + Zero injuries during evacuation process
2. **Communication During Rapidly Evolving Threat**
   * Objective: Maintain effective communication with all stakeholders as fire conditions change
   * SuccessCriteria:
     + Initial parent notification completed within 30 minutes of evacuation decision
     + Hourly updates provided through multiple channels
     + Coordination established with fire authorities within first hour
     + Rumor control measures implemented within 2 hours
3. **Transportation and Relocation Planning**
   * Objective: Safely transport and relocate students from threatened area
   * SuccessCriteria:
     + Transportation resources mobilized within 30 minutes
     + Safe relocation site(s) activated within 60 minutes
     + Special needs students accommodated with appropriate transportation
     + Reunification plan communicated to parents within 90 minutes
4. **Air Quality and Health Monitoring**
   * Objective: Protect student and staff health from smoke and air quality impacts
   * Success Criteria:
     + Air quality monitoring implemented at school and relocation sites
     + Medical needs of vulnerable students identified and addressed
     + Clear threshold criteria established for school operations
     + Proper documentation of health-related decisions maintained
5. **Extended Response and Recovery Planning**
   * Objective: Develop scalable response based on fire progression scenarios
   * Success Criteria:
     + Three-tiered plan developed for different severity scenarios
     + Essential functions maintained regardless of building status
     + Resources secured for 1-day, 1-week, and 3+ week scenarios
     + Regular reassessment of plans as fire situation evolves

Scenario

In late August, during the first week of school, a prairie fire ignites approximately 8 miles west of your K12 school campus. High winds and extremely dry conditions have led to a "Red Flag Warning" from the National Weather Service. The fire was initially small but has grown rapidly and is now approximately 3,000 acres. Local fire authorities report the fire is moving eastward (toward the school) at approximately 1-2 miles per hour due to 25-30 mph winds. The fire is currently 0% contained.

**Environmental Factors**

* Temperatures in the high 90s (°F)
* Relative humidity below 15%
* Wind gusts up to 35 mph
* No rainfall in the region for 6 weeks
* Smoke visible from school property
* Deteriorating air quality

**Impact to School**

* Potential threat to school facilities within 4-6 hours
* Declining air quality affecting outdoor activities
* High anxiety among students, staff, and parents
* Transportation routes potentially threatened
* Potential need for evacuation or early dismissal
* Possible multi-day closure depending on fire progress
* Smoke damage even if direct fire damage is avoided

**Timeline and Injects**

**10:15 AM** - Principal receives notification from county emergency management about wildfire

* Facilitator Details: The county emergency manager calls to inform the principal that a wildfire has started 8 miles west of the school. The fire is currently small but growing in high winds. No evacuation orders have been issued yet, but schools are advised to review emergency plans.
* *Inject 1*: Air quality index has moved from "Moderate" to "Unhealthy for Sensitive Groups"
  + Facilitator Details: Smoke is becoming visible in the distance, and local air quality monitors show worsening conditions. Several students with asthma have visited the nurse's office reporting difficulty breathing during morning recess.
  + Prompt Questions: What immediate actions should be taken regarding outdoor activities? At what air quality threshold should different activities be modified or cancelled? What provisions exist for students with respiratory conditions?
* *Decision Point:* Should normal school operations continue at this point?
  + Options to Consider:
    - Maintain normal operations with indoor recess/PE only
    - Cancel outdoor activities and athletic practices
    - Begin preparations for possible early dismissal
    - Initiate partial evacuation of vulnerable students
  + Discussion Guidance: Focus on balancing precautionary measures against disruption to educational activities, and the importance of staged responses to evolving threats.

**11:30 AM** - Fire officials issue "Pre-Evacuation Notice" for areas including school

* Facilitator Details: The fire has grown more rapidly than initially predicted due to high winds and extremely dry vegetation. It is now approximately 6 miles from the school and moving steadily eastward.
* *Inject 2:* Several parents arrive to pick up their children after seeing news reports
  + Facilitator Details: About 15-20 parents have come to the school without prior notice requesting to take their children home. The front office is becoming crowded, and additional parents are calling to ask if they should pick up their children.
  + Prompt Questions: What procedures should be followed for early student release during a potential emergency? How do you verify authorized pickups? How do you document which students have left with parents?
* *Inject 3:* Local news helicopter footage of the fire appears on social media
  + Facilitator Details: Dramatic aerial footage showing large flames and heavy smoke is being shared widely on Facebook and other platforms. Some posts include misinformation about evacuation orders already being in place for the entire community.
  + Prompt Questions: How do you counteract misinformation while still communicating appropriate urgency? What platforms should be monitored during the incident? Who is authorized to post official information on social media?

**12:15 PM** - Wind shifts, increasing rate of fire movement toward school

* Facilitator Details: Fire authorities report that winds have shifted and intensified, causing the fire to move more rapidly eastward. New projections suggest the fire could approach within 2-3 miles of the school by mid-afternoon.
* *Decision Point:* Do you initiate early dismissal, shelter in place, or evacuation to another site?
  + Options to Consider:
    - Early dismissal sending students home
    - Evacuation to predetermined alternate site
    - Shelter in place with enhanced air filtration
    - Partial solutions based on student transportation needs
  + Discussion Guidance: Consider the risks of each option, including transportation challenges, parental notification, and accounting for all students. Discuss the timing of decisions relative to fire progression.
* *Inject 4:* Transportation director reports three bus drivers are out of radio contact
  + Facilitator Details: The drivers were on field trips to different locations and radio communication is spotty. Cell phone service is becoming congested as more emergency calls flood the system.
  + Prompt Questions: What backup communication methods exist for bus drivers? How do you account for all staff and transportation assets during an emergency? What alternative transportation resources might be available?

**1:00 PM** - Mandatory evacuation order issued for areas within 5 miles of fire

* Facilitator Details: The county sheriff and fire incident commander have issued mandatory evacuation orders for a zone that includes the school. All personnel and students must leave the area within 60 minutes.
* *Inject 5:* Evacuation route options becoming limited as fire approaches
  + Facilitator Details: The primary evacuation route west is already closed due to fire activity. The southern route is reporting heavy traffic congestion as residents evacuate. The eastern and northern routes remain open but with increasing smoke conditions.
  + Prompt Questions: How are evacuation routes determined and communicated? What coordination occurs with law enforcement regarding traffic management? How are route changes communicated to bus drivers already in transit?
* *Inject 6:* Students expressing high anxiety and some panic during evacuation preparations
  + Facilitator Details: Some younger students are crying and expressing fear about the fire. Several older students are posting alarming content on social media, increasing anxiety. A few students are reporting they cannot reach their parents.
  + Prompt Questions: What emotional support resources are available during an evacuation? How do you balance speed with maintaining calm? What specific approaches work best for different age groups?

**1:45 PM** - School evacuation in progress

* Facilitator Details: Buses have arrived and evacuation of students is underway. Staff are conducting final building sweeps to ensure all students have been evacuated.
* *Inject 7:* Three students with mobility needs require specialized transportation
  + Facilitator Details: Two students use wheelchairs and one has crutches due to a recent injury. The specialized transportation van is currently off-site at a repair facility.
  + Prompt Questions: What accommodations exist for students with mobility challenges? Who is responsible for ensuring these students are safely evacuated? What backup plans should exist for specialized transportation?
* *Inject 8:* Parent reunification site reporting traffic gridlock
  + Facilitator Details: The predetermined reunification site at a church 7 miles east is experiencing severe traffic congestion as multiple schools and neighborhoods evacuate to the same general area. Parents are reporting 45+ minute delays reaching the location.
  + Prompt Questions: What criteria are used to select reunification sites? How are traffic management issues coordinated with local authorities? What communication should occur with parents facing delays?

**3:30 PM** - All students successfully evacuated; fire continues to approach

* Facilitator Details: All students have been evacuated to the designated reunification site, but only about 60% have been picked up by parents so far. The fire has reached a point approximately 2 miles from the school campus.
* *Inject 9:* Weather forecast predicts wind shift overnight
  + Facilitator Details: The National Weather Service issues an updated forecast indicating winds are expected to shift northward after midnight, which could potentially push the fire away from the school but toward residential areas where many students live.
  + Prompt Questions: How do changing forecasts affect planning for subsequent days? What criteria determine when it's safe to return to the building? How do you plan for students whose homes may now be threatened?
* *Decision Point:* How do you plan for school operations over the next 48 hours?
  + Options to Consider:
    - Full closure with no educational activities
    - Virtual learning if students have technology access
    - Consolidated operations at another district facility
    - Split/staggered schedule at an alternate location
  + Discussion Guidance: Discuss the factors that influence educational continuity decisions during an ongoing emergency, including community impact, resource availability, and duration uncertainty.

**Day 2 - 8:00 AM** - Fire officials report school not directly damaged but heavy smoke throughout area

* Facilitator Details: The fire line came within 1 mile of the school but did not directly damage the building. However, heavy smoke has infiltrated the building and surrounding air quality is in the "Hazardous" category on the AQI scale.
* *Inject 10:* Initial building assessment shows smoke damage to HVAC systems
  + Facilitator Details: Facilities staff report that smoke has permeated the HVAC system and the building interior has a strong smoke odor. Air filters are saturated, and ash has entered the building through various access points.
  + Prompt Questions: What assessment procedures should be conducted before reoccupying a building affected by smoke? What resources are needed for cleanup and air quality restoration? What standards determine when the environment is safe for students?
* *Inject 11:* Fire officials unable to predict when area will be safe for return
  + Facilitator Details: While the fire has moved beyond the immediate school area, it remains active and 10% contained. Officials cannot provide a definite timeline for when evacuation orders will be lifted.
  + **Prompt Questions**: What triggers the transition from emergency response to recovery operations? How do you communicate uncertainty to parents and staff? What phased return options might be appropriate?

**Day 3 - 1:00 PM** - School board emergency meeting to address ongoing closure

* Facilitator Details: The school board convenes to discuss extended closure impacts and options for educational continuity. The fire is now 30% contained but evacuation orders remain in place for the school zone.
* *Inject 12:* Environmental testing shows unsafe air quality levels inside building
  + Facilitator Details: Professional testing reveals particulate matter and volatile organic compounds within the building exceed recommended safety limits for children. Estimate for proper remediation is 10-14 days.
  + Prompt Questions: What health standards must be met before reoccupancy? Who makes the final determination that a building is safe? What documentation is required for insurance and compliance purposes?
* *Inject 13:* 25% of staff report they have been evacuated from their homes
  + Facilitator Details: A significant portion of school staff have been displaced from their homes due to fire evacuation orders or actual damage. Some have relocated temporarily to areas over an hour away.
  + Prompt Questions: How do you address staff needs while maintaining educational operations? What accommodations are appropriate for displaced staff? How might roles be temporarily modified during the emergency?
* *Decision Point:* What educational continuity plan will you implement for a 2+ week closure?
  + Options to Consider:
    - Secure alternative physical location(s)
    - Implement fully remote learning model
    - Create hybrid approach with satellite locations
    - Request emergency waiver for instructional time
  + Discussion Guidance: Explore the logistics, equity considerations, and resource requirements for each option. Consider how smoke and fire conditions affect the entire community, not just the school facility.

**Key Discussion Points**

1. At what point should outdoor activities be restricted based on air quality?
2. How do you coordinate evacuation decisions with emergency management officials?
3. What are the most effective parent notification methods during a rapidly evolving emergency?
4. How do transportation plans need to adapt when evacuation routes are compromised?
5. What special considerations exist for students with medical or mobility needs?
6. How do you balance early dismissal versus evacuation to another site?
7. What criteria determine when it's safe to reoccupy a building after smoke exposure?
8. How do you address the emotional impact on students, staff, and families?
9. What mutual aid agreements exist with other districts for emergency support?
10. How are parent reunification procedures managed during a community-wide evacuation?
11. What ongoing communication is needed during a multi-day emergency?
12. How do air quality standards influence educational environment decisions?

Facilitator Background Information

**Wildfire Behavior and Terminology**:

* Fire behavior depends on three primary factors (the "fire triangle"):
  + Fuel (vegetation type, density, and moisture content)
  + Weather (wind, temperature, humidity)
  + Topography (slope, aspect, terrain features)
* Key terms participants should understand:
  + Containment: Percentage of the fire perimeter that has a control line around it
  + Spot fires: New fires ignited by embers blown ahead of the main fire
  + Rate of spread: Speed at which the fire is moving (typically feet/chains per hour)
  + Red Flag Warning: Weather conditions that support extreme fire behavior
  + Backburn/burnout: Intentionally set fires to consume fuel in the path of a wildfire

**Air Quality Considerations for Schools**:

* Air Quality Index (AQI) categories and recommended actions:
  + 0-50 (Good): Normal activities
  + 51-100 (Moderate): Unusually sensitive students should limit prolonged outdoor exertion
  + 101-150 (Unhealthy for Sensitive Groups): Keep sensitive students indoors
  + 151-200 (Unhealthy): Move all activities indoors, close windows, limit physical exertion
  + 201-300 (Very Unhealthy): Consider school closure or relocation
  + 301+ (Hazardous): School closure strongly recommended
* HVAC considerations:
  + Recirculation mode should be used during smoke events
  + MERV 13+ filters can capture most smoke particles
  + Portable air purifiers with HEPA filters can create clean air spaces
  + Building pressurization helps prevent smoke infiltration

**Evacuation Decision Factors**:

* School evacuation decisions should consider:
  + Time available before threat arrives
  + Transportation resources and routes available
  + Reunification capabilities
  + Special needs of student population
  + Shelter availability
  + Duration of expected displacement
  + Community evacuation orders and traffic
* Evacuation alternatives include:
  + Shelter-in-place with enhanced protective measures
  + Early dismissal (when homes are safe)
  + Partial evacuation of vulnerable populations
  + Full evacuation to predetermined locations

**Recovery and Reoccupancy Standards**:

* Key factors for determining building reoccupancy include:
  + PM2.5 levels below 35 μg/m³ (EPA standard)
  + CO, CO2, and VOC levels within normal ranges
  + HVAC system cleaned and filters replaced
  + Absorbent materials (carpet, curtains, etc.) properly cleaned
  + No visible ash or soot remaining
  + Odor remediation completed
  + Air monitoring shows stable, acceptable air quality

# BONUS CONTENT: Making Mini Tabletop Exercises into Micro Moments

**Focus on One Decision Point**

Instead of running the full scenario, select a single inject or key decision (e.g., "Ransom demand received—who do you notify first?") and talk it through.

Tip: Use sticky notes or a whiteboard to map quick answers.

**Use "What If" Prompts**

Turn news headlines or real-life incidents into a quick challenge:  
“What if a student received a ransomware text message today—what would you do in the first 10 minutes?”

Trick: Encourage “gut reactions,” then reflect on how to improve the plan.

**Build Weekly or Monthly Habits**

Schedule a standing 5-minute “resilience rep” in weekly IT meetings. Choose a topic in advance, rotate facilitators, and tie it to recent incidents or seasonal risks.

**Use Role Cards for Quick Immersion**

Hand out simple role cards (Principal, IT Director, Nurse, Parent) and ask: “From your role, what’s your biggest concern in this moment?”

Bonus: Helps staff empathize across functions and understand interdependencies.

**Simplify with the 3-3-3 Formula**

For ultra-micro drills:

* 3 Minutes: Present a trigger (e.g., “Backup failed last night—go!”)
* 3 Questions: Ask who, what, and how.
* 3 Takeaways: End with agreed-on action steps or gaps to investigate.

**Use “Sticky Scenarios” on Shared Boards**

Place a dry-erase board or virtual board in the staff room or Teams channel with a weekly “sticky scenario.”  
Invite short written responses—no meeting required!

**Gamify It!**

Turn responses into a challenge:  
✔️ Fastest correct response  
🏅 Most creative workaround  
🔥 “That would totally happen” real-life example

**Tie Every Micro to One of the Five Plans**

Always anchor the micro-exercise in one of your critical planning areas:

* Crisis Management
* Crisis Communication
* Cyber Incident & Disaster Response
* Educational Continuity
* Technology Recovery

Trick: Use color-coded icons or cards to make this visible.

Micro Exercise Seasonal Risk Calendar

|  |  |  |
| --- | --- | --- |
| Month | Seasonal Focus | Micro Exercise Idea |
| August | New Staff Onboarding & Phishing Threats | Simulate a fake email or credential scam targeting new hires. |
| September | System Overload & Data Entry Errors | Test response to incorrect student health or contact information. |
| October | Cybersecurity Awareness & Ransomware | Run the ransomware micro tabletop with twist cards. |
| November | Weather Closures & Communication Failures | Practice communication plans for a sudden blizzard-related closure. |
| December | Student Wellness & Privacy | Simulate a mental health crisis with privacy/FERPA implications. |
| January | Cold Weather Facility Disruptions | Respond to frozen pipes or HVAC failure with students in the building. |
| February | Vendor Breaches & SIS Dependencies | Micro tabletop on vendor system breach affecting assessments. |
| March | Spring Storms & Early Flooding | Test shelter-in-place or early dismissal communication during storms. |
| April | Standardized Testing Interruptions | Run a scenario on LMS outage or lost testing data. |
| May | Device Turn-In & Data Wipe Mistakes | Respond to accidental deletion of student records during device cleanup. |
| June | Summer Project Risks & Backup Validation | Test your data backup validation and summer upgrade disaster planning. |
| July | Contractor Access & Security Gaps | Simulate unauthorized access during summer construction or IT upgrades. |