Nebraska Schools Cybersecurity Breach: Tabletop Exercise

Situation Manual

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

Funding for this exercise was made possible, in part by S184Q18009-18A from the U.S. Department of Education.

Exercise Overview

Exercise Name	Nebraska Schools Cybersecurity Breach
Exercise Dates	
Scope	This exercise is a workshop planned for 1.5 hours. Exercise play will include facilitated participant discussion.
Mission Area(s)	**Protection, Prevention, and Preparedness, Response**
Core Capabilities	Public Information and Warning Critical Transportation Cybersecurity Intelligence and Information Sharing Operational Coordination Operational Communications
Objectives	Test coordination of school anti-virus resources and collaboration among information technology assistance. Identify information technology resource issues and opportunities. Ensure capacity for accurate and timely communication in support of operations and Clearly communicate details of the incident with staff, parents, and the community. Test plans for transporting students in case of a virtual attack, crippling infrastructure
Threat or Hazard	Cybersecurity Breach

Exercise Name	Nebraska Schools Cybersecurity Breach
Scenario	There are two scenarios. In scenario one, schoolteachers open an email from their superintendent regarding necessary updates from human resources to receive their next paycheck. The link is indeed fraudulent but results in personal information being obtained by the hacker. In scenario two, a ransomware attack on the district's servers hacked encrypted data and crippled the district's infrastructure. The hackers are demanding $30,000 to take down the ransomware. Because of the seriousness, school has been canceled for two days.
Sponsor	Nebraska Department of Education; University of Nebraska Public Policy Center
Participating Organizations	Nebraska Department of Education; University of Nebraska Public Policy Center; local Nebraska Educational Service Units (ESUs); local Nebraska school officials/staff/faculty
Point of Contact	Denise Bulling, PhD University of Nebraska Public Policy Center 215 Centennial Mall South, Suite 401 Lincoln, NE 68588 402-472-1509

General Information

Exercise Objectives and Core Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s). The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

Exercise Objectives	Core Capability
Test coordination of school cybersecurity (anti-virus) resources and collaboration among information technology assistance.	Operational Coordination
Identify information technology resource issues and opportunities.	Cybersecurity
Ensure capacity for accurate and timely communication in support of operations	Operational Communication
Clearly communicate details of the incident with staff, parents, and the community.	Public Information and Warning
Test plans for transporting students in case of a virtual attack, crippling infrastructure	Critical Transportation

Table 1. Exercise Objectives and Associated Core Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers:** Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitators:** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Evaluators:** Evaluators are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise will be a multimedia, facilitated activity that can be conducted in person or in Zoom. Players will participate in the following scenarios:

- Scenario 1: A phishing attack directed at schoolteachers.
- Scenario 2: A district-wide ransomware attack cripples the district's infrastructure and jeopardizes student and staff data.

Participants review the situation and engage in group discussions. After these discussions, participants will engage in a moderated plenary discussion in which a spokesperson from each group will present a synopsis of the group's actions based on the scenario.

Exercise Guidelines

- This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent-setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve response and recovery efforts. Problem-solving efforts should be the focus.

Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise and should not allow these considerations to impact their participation negatively.

- The exercise is conducted in a no-fault learning environment wherein capabilities, plans, systems, and processes will be evaluated.
- The exercise scenario is plausible, and events occur as they are presented.
- All players receive information at the same time.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned capabilities, capability targets, and critical tasks, which are documented in Exercise Evaluation Guides (EEGs). Evaluators have EEGs for each of their assigned areas. Additionally, players will be asked to complete participant feedback forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and inform any After-Action Reports (AAR).

Scenario 1: Phishing Attack

District schoolteachers open an email from the superintendent asking them to update Social Security numbers, bank account information because Human Resources is “upgrading” its employee direct deposit system. The email notes that if recipients fail to provide their sign-in credentials and updated information immediately they would not receive their upcoming paycheck on time. Within the email is a link that prompts them to log into their account. District staff is accustomed to receiving emails from the superintendent regarding school updates, human resource issues, and training opportunities, so this email is nothing new.

For most teachers, an internal red flag is raised, and they verify the fraudulent email by reporting it to their IT department. But a few teachers go ahead and follow the link, resulting in the hacker obtaining personal information (namely Social Security numbers and bank account information).

Key Issues

- Phishing/Spoofing
- Cybersecurity
- Personal data loss

Questions

1. Consider Information Technology support. Who are your district IT professionals? Who would you call in this situation? How would they be able to help you?

2. What type of training for students, faculty, and staff on cybersecurity best practices might help prevent this situation? Does your district offer this type of training? What other strategies might prevent phishing attacks?

3. What other strategies can help prevent, protect against, and mitigate the effects of phishing and other types of cyber threats?

4. Consider insurance. Does your school carry cyber insurance policies? If so, who and what does the policy cover? Cyber insurance policies can help pay legal fees, credit monitoring services for those impacted by the breach, and financial losses.

5. What are your communication strategies? How do you notify teachers and other school staff? within the district/school? Do you notify parents and the community? If so, what information do you provide?

Scenario 2: Ransomware Attack

A ransomware attack on the district's servers hacked encrypted student data that included schedules, demographic information, contact information, assignments, grades, and medical information. The outage has also affected infrastructure, including bus routes, nutrition systems, security cameras - even teacher's badges will not let them into their buildings. The network loss prohibits teachers from electronically taking attendance, assigning grades, giving assignments, and so on. As a result, leadership is forced to close school until administration, IT professionals, and the state department of education figure out a solution.

The hackers are demanding $30,000 to take down the ransomware, or they will start making this information public. As a scare tactic, they have already released some low-level information through various media outlets sparking outrage among the community. Parents are furious because they have to make alternate care plans for their children and are worried about their personal information being compromised.

Key Issues

- Ransomware
- Cybersecurity
- Massive data loss

Questions

1. How will the district respond to the loss of critical student data until the information can be recovered? What if it is never recovered?

2. With regard to the ransom, do you pay it in hopes that the information will be returned to the school? What are the implications of making this payment? How would you pay it? Consider any precedents for schools paying such a ransom.

3. In the event that the cyber security attack lasts multiple days and school servers are down, what is your policy for school attendance?
    a. When deciding if school is to remain in session, what factors would change this outcome?
    b. How do you communicate this with school staff, students, parents, and community members?

4. What steps can you take now to ensure that cyber attacks at your school or district are minimized?

Definitions:

Spoofing refers to the dissemination of an email that is forged to appear as though it was sent by someone other than the actual source.

Phishing is the act of sending an email falsely claiming to be a legitimate organization in an attempt to deceive the recipient into divulging sensitive information (e.g., passwords, credit card numbers, or bank account information) after directing the user to visit a fake website.

Ransomware is form of malware in which perpetrators encrypt users' files, then demand the payment of a ransom—typically in virtual currency such as Bitcoin—for the users to regain access to their data.