[Enter Organization Name]

CISA Tabletop Exercise Package – K-12 Schools

<Exercise Date>

Table of Contents

Handling Instructions

Delete instructions that are not applicable.

The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries that are applied to the recipient(s) of the information.[1] Select one of the following TLP designations below for this CISA Tabletop Exercise Package based on your information sharing needs.

TLP: WHITE

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):WHITE*": Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.**

This document may be disseminated publicly pursuant to TLP:WHITE and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP: GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):GREEN*": Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP:GREEN information may not be released outside of the community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP: AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):AMBER*": Limited disclosure, restricted to

[1] CISA Traffic Light Protocol (TLP) definitions and usage. Retrieved 8 December 2021 from https://www.cisa.gov/tlp.

participants' organizations. This designation is used when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP: RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):RED*": Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, **TLP:RED should be exchanged verbally or in-person**.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

Exercise Overview

Exercise Name	Exercise Name	
Exercise Date, Time, and Location	Exercise Date Time (e.g., 9:00 a.m. – 12:00 p.m.) Exercise Location	
Exercise Schedule	**Time**	**Activity**
	Time	Activity
	Time	Activity
	Time	Activity
	Time	Activity
Scope	X hour facilitated, discussion-based Tabletop Exercise	
Purpose	Improve <name of school or district>'s cybersecurity program awareness, plans, decision making process, and capabilities in response to a cyber threat-based scenario.	
NIST Framework Functions	For example, areas such as Identify, Protect, Respond, etc.	
Objectives	1. Increase cybersecurity program awareness and engagement among school stakeholders. 2. Assess the viability of <name of school or district>'s cyber incident response in the event of a significant cybersecurity incident. 3. Explore <name of school or district>'s cybersecurity information sharing protocols with internal and external stakeholders. 4. Examine <name of school or district>'s internal and public communications roles, responsibilities, and procedures in response to a cybersecurity incident.	
Threat or Hazard	Cyber Threats	
Scenario	A threat actor targets <your school / district> employees through phishing emails. Ransomware compromises the computer system with multiple impacts including exfiltration of students' Personally Identifiable Information (PII), loss of school heating, ventilation, and air conditioning (HVAC) system control, and media inquiries.	
Sponsor	Exercise Sponsor	
Participating Organizations	Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.)	
Points of Contact	**Insert Organization POC(s)** Contact info	**CISA Exercises** CEP@hq.dhs.gov

General Information

Exercise Guidelines

- This exercise will be held in an open, no-fault environment. Varying viewpoints are expected.
- Respond to the scenario using your knowledge of existing plans and capabilities, and insights derived from your training and experience.
- 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 and/or suggested actions to resolve or mitigate a problem.
- There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
- The scenario has been developed in collaboration with subject matter experts and exercise planners from your organization.
- In any exercise, assumptions and artificialities are necessary to complete play in the time allotted, to achieve training objectives, and/or account for logistical limitations. Please do not allow these considerations to negatively impact your participation in the exercise.

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 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 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 provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.
Note-takers are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise will be a multimedia, facilitated exercise. Players will participate in the following:

- Cyber threat briefing (if desired)
- Scenario modules:
  - **Module 1:** A cybersecurity alert for K-12 institutions, teachers who do not change the default password on school-issued laptops, the contentious firing of a staff member, and a phishing email.
  - **Module 2:** A ransomware attack affecting school networks, media inquiries, and data exfiltration affecting student records.
  - **Module 3:** Additional media interest and ransomware demands.

- ***Structure Note:*** *Injects and discussion questions included in each module may be modified as desired. This exercise has been designed to explore several different threats to your organization, indicated in bold parentheses before the inject text. Your organization may select specific types of events and threats for your exercise and should delete any extra injects and discussion questions not relevant to your selected scenario. Additional discussion questions can be found in Appendix A.*

Exercise Hotwash

The facilitator will lead a hotwash with participants at the end of the exercise. The hotwash is an opportunity for exercise participants to discuss the strengths and weaknesses of their organization's response to the events presented during the exercise to address any ideas or issues that emerge from the exercise discussion.

Module 1

Day 1

The Cybersecurity Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issue a joint alert regarding a rise in cyberattacks targeting K-12 educational institutions. The alert describes the tactics, techniques, and procedures (TTPs) used by cyber criminals, including phishing emails, ransomware, remote hacking, distributed denial of service (DDoS) attacks, and data exfiltration from schools and distance learning providers. Cyber threat actors view schools as targets of opportunity and these attacks are expected to continue through the <20XX-20XX> academic year.

Day 7

A staff member is fired for being late to work multiple times at the beginning of the school year. The staff member makes a public and unprofessional commotion while leaving the building.

Day 9

An urgent email claiming to be from Human Resources instructs employees to update their banking information in <your district> payroll system. The email states that employees who fail to update their information will not receive their next paycheck on time. When users click the email link, it takes them to a page that looks like the <your district> website and prompts them to log in using their employee credentials.

Day 10

Take-home laptop devices are issued to students and teachers at <your school's name>. Teachers pick up their designated laptop and begin setting up their classrooms. A few teachers use the default passwords rather than creating their own.

Day 30

As the school year continues, teachers routinely access their email accounts and save student grades and personally identifiable information (PII) on their laptops and on a cloud-based platform.

Discussion Questions

Your organization may select specific types of events and threats for your exercise and should delete any discussion questions not relevant to your selected scenario. Additional discussion questions for each module can be found in Appendix A.

1. What is the greatest cybersecurity threat to <your school or district>?
    a. What process do you use to assess cyber risks for <your school or district>?
2. What essential school functions depend on information technology and what are the cascading effects of their disruption?
3. What cybersecurity threat information does <your school or district> receive?
    a. What actions would <your school or district> take based on this information?
3. How would you describe <your school/district's> cybersecurity posture?
    a. How frequently are users required to change their passwords?

   b. Does <your school district/county> utilize multi-factor authentication (e.g., something you know, something you have, something you are) to mitigate the potential effects of phishing?

4. What is your onboarding and offboarding processes for employee network access?
5. Describe <your school/district's> cybersecurity training program.
   a. How frequently do employees receive cybersecurity training?
   b. What cybersecurity training does <your school/district's> provide students and/or parents?
   c. What are your training requirements for third-party vendors or external personnel who access your network/systems?
6. How do users report suspicious emails?
   a. What procedures or plans would be followed once a suspicious email has been reported?

Module 2

Day 45

Following the most recent pay date, a report from Human Resources indicates that 38 employees did not receive their paychecks, despite having up-to-date account information and enabling direct deposit for their accounts.

IT staff receive an unusually high number of reports from faculty and staff who are unable to access their employee accounts. Staff members are seeing error messages that their credentials are invalid, or their account no longer exists in the system.

Day 46

Faculty and staff who are still logged in to the system cannot access their school emails, curriculum materials, and student grades on their local drives or the online school platform. They are presented with the following message on their devices:

"We own your data. For $350,000 in Bitcoin, your files will be returned. Submit payment to the wallet below within 96 hours, or everything will be posted for sale to the highest bidder. Don't believe us? We will publish some of your data every 24 hours."

Day 47

The <IT Director or equivalent position> for <school district/county> confirms the incident and says that the IT staff is working to solve the issue as quickly as possible.

Day 48

The attackers publish a sample of exfiltrated student data from your school on a hacker forum. They also claim they will release more data every 4 hours until the ransom is paid.

A social media post begins trending with #SchoolHacked and a screenshot of the hacker forum. The screenshot includes student names, telephone numbers, and addresses from <name of school>. Parents of the listed students angrily call the school, and many want to involve local law enforcement.

Discussion Questions

Your organization may select specific types of events and threats for your exercise and should delete any discussion questions not relevant to your selected scenario. Additional discussion questions for each module can be found in Appendix A.

1. What are your priorities based on the events in Module 2?
2. What actions would your <school district/county> take to minimize the incident's impact on current school operations?
    a. How long can you maintain alternative procedures for student instruction (e.g., virtual learning)?
    b. When would you consider instructing students not to use school-issued devices?
    c. What backups do you have to facilitate school system recovery and how often are they tested?
    d. How long would it take to recover and restore impacted systems?

3. What actions would be taken based on <your school district/county's> incident response plan?
    a. What ransomware policies and procedures are included in your incident response plan?
    b. What does <your school district/county's> cyber insurance policy cover?
4. What is the decision-making process for ransomware payment?
    a. How are your cyber insurance providers involved in your procedures?
    b. What are the advantages/disadvantages to agreeing/refusing to pay?
    c. What are the potential legal and reputation ramifications?
5. What is your threshold for contacting law enforcement during a cyber incident?
6. What concerns would arise with the discovery of sensitive and/or personal information of students being available online?
    a. How does <your school district/county> monitor social media?
    b. How would <your school district/county's> Public Information Officer respond to the social media posts and parent complaints?

Module 3

Day 49

All parents/guardians receive an email from their student's teachers with an attachment that includes the grades of every student in their class and the message: "Worst teacher ever!!"

Students report that their upcoming homework assignments have been deleted from their online drive. Teachers also notice different students are submitting multiple identical copies of their homework assignments.

Day 50

The hacker group "Morning Avengers" announces that they have taken control of <your school> in a social media post and demands an additional $250,000 in Bitcoin.

Faculty and staff notice that the classrooms are getting hotter, and maintenance staff cannot adjust the temperature.

Day 51

Your local news outlet calls <your school> asking for comments on the ransomware incident and impacts to student learning. Several parents/guardians have been interviewed by the news outlet and express concerns for their students' safety.

Discussion Questions

Your organization may select specific types of events and threats for your exercise and should delete any discussion questions not relevant to your selected scenario. Additional discussion questions for each module can be found in Appendix A.

1. What are your priorities based on the events of Module 3?
2. What are your concerns regarding the loss of temperature control?
3. How would the increased ransom demand affect your decision-making regarding the ransomware payment?
4. When would a cyber incident prompt you to plan for changes to the academic calendar?
5. What communications plan does <your school district/county> public information office have for responding to cyber incidents?
    a. How will you ensure continuity of information being shared with staff, parents/guardians, and students?
    b. How would <your school district/county> address these incidents with the local media?
6. How sufficient are <your school district/county's> current internal resources for responding to the cyber incidents in this scenario?
    a. What additional resources would you need and what is the process for requesting them?

Appendix A: Additional Discussion Questions

The following section includes supplemental discussion questions to guide exercise play. Questions are aligned to the NIST functional areas, specific attack vectors, and roles. Exercise planners are encouraged to select additional, applicable discussion questions to the chosen scenario to bolster participant conversation. *This instructional page, as well as undesired discussion questions, should be deleted.*

Cyber Preparedness and Planning

1. How does <your school district/county's> incident response plan aid in the mitigation of the cyberattacks presented?
2. What level of funding and/or resources are devoted to cyber preparedness?
3. Based on <your school district/county's> risk assessment, what is the range of potential losses from a cyber incident?
4. Discuss cyber preparedness integration with your current all-hazards preparedness efforts.
5. Who are <your school district/county's> cyber preparedness stakeholders (public, private, non-profit, other)?
6. Who oversees cybersecurity management?
7. How are background checks conducted for IT, security, and key supporting personnel?
8. What precautions does <your school district/county> take against cyber threats?
9. How well-defined is cybersecurity in relation to contracts with third-party support vendors and crucial suppliers?
    a. How often are contracts reviewed?
    b. How well do <your school district/county> service level agreements address incident response?
10. What protections does <your school district/county> have to defend against malicious intent by vendors or outside parties that have access to your network?
11. What are <your school district/county>'s formal or informal procedures pertaining to IT account management?
    a. Do these procedures include protocols for establishing, activating, modifying, disabling, and removing accounts?
    b. What is <your school district/county> process for disabling accounts and network access of former employees that were recently terminated or voluntarily resigned?
12. How does <your school district/county> baseline network activity?
    a. How would <your school district/county> be able to distinguish between normal and abnormal traffic?
13. What type of hardware and/or software does <your school district/county> use to detect/prevent malicious activity of unknown origin on <your school district/county> systems/network?
14. What is the procedure for deploying high priority patches of user applications and software?
15. What is the process for students and parents/guardians to report suspicious cyber incidents?
16. What current IT processes address these types of cyber incidents?
17. How are employees trained to recognize and report cyber threats such as phishing scams?
    a. Does <your school or district> require additional training for those who fall for a fake phishing campaign?

18. What is the password management policy for <your school district/county> local or internal network?
19. How regularly are users required to change their passwords?
    a. What is <your school district/county's> account lockout policy if users don't change their passwords in a timely fashion?
    b. What are <your school district/county's> requirements for password length and level of complexity?

Information Sharing

1. What established mechanisms does <your school district/county> have to facilitate rapid information dissemination?
    a. What are <your school district/county> known communication gaps? Who in <your school district/county> is responsible for addressing those gaps?
2. What other sources of cybersecurity threat intelligence does <your school district/county> receive (e.g., information from FBI, MS-ISAC, open-source reporting, security service providers)?
    a. What cyber threat information is most useful?
    b. Is the information you receive timely and actionable?
    c. Who is responsible for collating information across <your school district/county>?
3. How is information shared among <your school district/county> internal and external stakeholders?
    a. What formal and informal information sharing mechanisms are in place?
4. What mechanisms and products are used to share cyber threat information within <your school district/county> and external to <your school district/county> (e.g., distribution lists, information sharing portals)?
5. Describe how variables in threat information (timeframe, credibility, and specificity) impact decision making.
6. What flowcharts showing the high-level relationships and crisis lines of communication (i.e., who calls who) does <your school district/county> have for a cyber incident?
    a. Are they part of <your school district/county's> response or continuity planning documents?

Incident Response

1. When was <your school district/county>'s cybersecurity incident response plan issued and when was the plan last revised?
2. Does <your school district/county> incident response plan identify who to contact if you suspect you have experienced a cyber incident?
3. What is <your school district/county> method for tracking and/or identifying problematic pieces of firmware in <your school district/county>, if a vulnerability is identified?
4. When do <your school district/county> IT and helpdesk staff conduct network maintenance (e.g., specific days or times of day)?
5. What is <your school or district> IT department's patch management plan?
    a. Are risk assessments performed on all servers on the network?
    b. Are there processes to evaluate each server's criticality and applicability to software patches?
6. What resources and capabilities are available to analyze an intrusion or mitigate the incident?

   a. Internally?
   b. Through the private sector (third party vendors)?
   c. Through government partners?
7. Describe the decision-making process for protective actions in a cyber incident.
   a. What options are available?
   b. Have these options been documented in plans?
   c. How are they activated?
8. What immediate protection and mitigation actions would be taken at <your school district/county> in this scenario? Who is responsible for those actions?
9. What detection methods does <your school district/county> have to identify a compromise?
10. What protective actions would <your school district/county> take across non-impacted systems in the scenario presented?
   a. Who is responsible for protective action decision-making?
   b. How are actions coordinated across parts of <your school district/county>?
11. How would you rate this security incident severity for <your school district/county>? What additional notifications or actions would this prompt?
12. Describe whether this scenario exceeds <your school district/county's> ability to respond.
   a. If so, what are <your school district/county's> established procedures to request additional support?
13. Who does <your school district/county> receive cyber response technical assistance from?
   a. Does <your school district/county> have plans and procedures in place to access this assistance?
14. Has <your school district/county> identified and established the service provider relationships needed for incident/breach response issues (e.g., credit counseling, forensic/computer security services)?
   a. What are some challenges that are experienced by information technology and business continuity planning in terms of information sharing?
   b. Is information flowing in both directions?
15. What processes are used to contact critical personnel at any time, especially outside of business hours?
   a. How does <your school district/county> proceed if critical personnel are unreachable or unavailable?
16. What alternative systems or manual processes are available to continue operations if a critical system is unavailable for a significant period?
   a. Who can authorize use of alternate systems or procedures?
17. When and how does <your school district/county> determine a cyber incident is closed?
18. What are <your school district/county>'s defined cybersecurity incident escalation criteria, notifications, activations, and/or courses of action?
   a. Where does this incident fall within the incident severity schema for <your school district/county>?
   b. When would <your school district/county> leadership be notified?
   c. When would <your school district/county> Board of Education (BOE) be informed of the cybersecurity incident?
19. When would <your school district/county>'s cyber incident response team be activated?
   a. What are their priorities?

   b. Does <your school district/county> BOE have a role on the cyber incident response team?
20. What incident de-escalation procedures are in place?
   a. Has <your school district/county> established a quantifiable, repeatable process for determining when an incident is resolved and when the incident response team can stand down?
21. Describe <your school district/county>'s After Actions Report or lessons learned process.
   a. Who leads this process for a cyber incident?
   b. How are recommended improvements implemented and tested?
22. What remediation is required of employees to ensure an event like this does not happen again (training, self-education, etc.)?

Ransomware

1. What resources are required for incident investigation and attribution?
2. When have other schools or districts notified <your school district/county> after detecting a ransomware attack?
   a. If they have not notified <your school district/county>, should they?
3. When would <your school district/county> notify other schools or other districts in your area after a ransomware attack is detected?
4. If you were one of the individuals who received the ransom demand, who would you inform, internally? Who would you inform externally?
5. How is ransomware addressed in <your school district/county> incident response plan?
   a. How frequently does <your school district/county> exercise your response to ransomware?
6. What formal policies and procedures does <your school district/county> have to document the process for restoring backed-up data?
   a. Do these policies and procedures include measures for ensuring the integrity of backed-up data before restoration?
7. Where does <your school district/county> store back-ups of vital records?
   a. Are your backups stored in a location that is separated from your primary working copies of your files?
   b. How long does <your school district/county> keep any copies of archived files backed up?
   c. How long of a downtime would exist between loss of your primary files and the restoration of files via your back-up?
8. How would <your school district/county> respond to the loss of student transcripts and test scores?
   a. Who would be involved in the response?
   b. Who would be notified at the local level? State level? Federal level?
9. What processes and resources are used for evidence preservation and forensics?
   a. When would <your school district/county> engage law enforcement, if at all?
   b. Who would <your school district/county> be contacting from local, state, and federal entities?
10. What steps would be taken to regain access to locked accounts?

   a. Do employees know who to contact in this situation?

11. What is <your school district/county>'s responsibility to provide credit monitoring or other identity theft protection services for individuals affected by the stolen data?
12. In addition to the concerns of data exfiltration, how would <your school district/county> address incorrect data in student records?

Phishing

1. How do employees report suspected phishing attempts?
   a. What actions does <your school district/county> take when suspicious emails are reported?
   b. Are there formal policies or plans that would be followed?
   c. Does <your school district/county> conduct phishing self-assessments?
2. How are students notified of possible phishing campaigns targeting their accounts?
   a. How would parents/guardians be involved in this conversation?
3. Does <your school district/county> provide basic cybersecurity and/or IT security awareness training to all users (including managers, senior executives, and vendors)?
   a. What topics does the training cover and how often is it provided?

Data Exfiltration

1. How would <your school district/county> be notified if data exfiltration occurred in a neighboring school or district?
2. What actions would be taken when the exfiltration is discovered? Does <your school district/county> have written plans that would be implemented?
3. What impact will the potential sale of students' sensitive or Personally Identifiable Information (PII) have on <your school district/county> response and recovery activities?
   a. Will IT alert authorities?
   b. How have <your school district/county> public relations priorities changed?
   c. Will it trigger any additional legal or regulatory notifications?

Distributed Denial of Service

1. How does <your school district/county> detect and mitigate the effects of DDoS attacks?
   a. Does <your school district/county> contract with a vendor for DDoS protection?
   b. Who can activate the DDoS protections? (Standard services should be on all the time; however, some advance features are activated based upon attack type and severity.)
   c. What processes and procedures does <your school district/county> have to notify the vendor that <your school district/county> is under a DDoS attack?
   d. How are these processes and procedures documented in <your school district/county>'s incident response plan?
2. How has <your school district/county>tested or exercised the DDoS detection and mitigation capabilities?
3. What active measure(s) does <your school district/county> employ to prevent denial of service (DDoS) attacks against your websites and operational systems?

4. What pre-written messages does <your school district/county> have to inform faculty, staff, students, and parents/guardians of a DDoS attack?
    a. Does this messaging include actions they should/should not take?

Public Affairs

1. What steps would be taken to address the public following these cyber incidents?
    a. Is there a forum for parents to ask questions?
    b. How would students be notified about the cyberattacks?
2. Who is responsible for public information dissemination related to the incident? What training or preparation have they received?
3. Does the public relations team have a dedicated list of individuals to contact in the event of an incident? Who is on that list? Are those offices/individuals listed in any order of priority?
4. How is <your school district/county> ensuring unity of message between <your school district/county>, the public partners, and elected officials?
5. What online resources and communication formats does <your school district/county> use to keep parents, students, and the public informed regarding any incidents?
6. How would <your school district/county> public information office work jointly with other public relations offices/ departments in local, state, and federal government to ensure a consistent message is being delivered to the public?

Legal

1. What are the legal issues <your school district/county> must address?
2. What legal documents should <your school district/county> have (for example with third-party vendors)?
    a. Discuss the role of cybersecurity in contracts with third-party support vendors and crucial suppliers. Has <your school district/county> discussed cybersecurity concerns and risks with them?
3. What is the role of the legal department in this scenario?
4. What are <your school district/county> security breach notification laws? What do they include?

Appendix B: Acronyms

Acronym	Definition
AAR	After-Action Report
BOE	Board of Education
CISA	Cybersecurity and Infrastructure Security Agency
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
FBI	Federal Bureau of Investigation
HVAC	Heating, Ventilation, and Air Conditioning
MS-ISAC	Multi-State Information Sharing & Analysis Center
IS	Information Systems
IT	Information Technology
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
TLP	Traffic Light Protocol

Appendix C: Case Studies

Distributed Denial of Service

Miami-Dade County Public Schools (MDCPS) DDoS

In September 2020, MDCPS suffered DDoS attacks on their first day of distance learning that prevented 20,000 teachers and 275,000 students from accessing the online portal for remote learning. The DDoS attacks rendered multiple online school district features useless and teaching nearly impossible for the first three days of the school year. MDCPS contacted the Federal Bureau of Investigation and U.S. Secret Service to investigate. Investigators determined that a sixteen-year-old student collaborated with foreign actors to purchase and use a Low Orbit Ion Cannon (LOIC) to attack the schools' network. Some teachers and students, who were unaware of the DDoS attack, were able to transition to Zoom or other MDCPS platforms to continue learning activities.[2]

Winthrop Public Schools DDoS

In February 2020, Winthrop Public Schools, a school district in Massachusetts, had their Google Classroom, email, and video conferencing taken offline during a DDoS attack on the town of Winthrop's servers. The DDoS attack disrupted service in school and town buildings, but no employee or student information was accessed during the incident. Officials worked to restore service and the schools were able to keep their hybrid class schedule, with some students attending in person while others participated in remote learning.[3]

Ransomware

Baltimore County Public Schools (BCPS) Ransomware

In November 2020, BCPS, a school district in Baltimore County, MD, was forced to cancel online classes for 115,000 students after a ransomware attack impacted email, grading, and some study material meant to be distributed among students. The BCPS official school website was taken down because of the attack and students and teaching staff were given time off until the incident was resolved. The district announced that it intended to recover its data from backups and told students not to use school-issued Windows-based devices until further notice. Student transcripts, ID numbers, state test scores, and more information stored in the Student Information System were

[2] Ari Odzer, T. P. (2020, September 3). *Student Arrested in Connection With Cyberattacks on Miami-Dade Public Schools*. Retrieved from NBC Miami: https://www.nbcmiami.com/news/local/student-arrested-in-connection-with-cyberattacks_-on-miami-dade-public-schools/2287613/; Wadhwani, S. (2020, September 3). *DDoS Attacks Plague Miami-Dade County Public Schools*. Retrieved from https://www.toolbox.com/security/network-security/news/ddos-attacks-plague-miami-dade-county-public-schools/.

[3] Bonner, Michael (2021, February 5). *Winthrop Public Schools, town offices targeted in cyber-attack which prevented access to Google Classroom, email, video conferencing*. Retrieved from MassLive: https://www.masslive.com/boston/2021/02/winthrop-public-schools-town-offices-targeted-in-cyber-attack-which-prevented-access-to-google-classroom-email-video-conferencing.html

apparently destroyed, slowing the district's recovery. Reports indicate the school district paid $6 million to help pay for the damage caused by the attack.[4]

Huntsville City Schools Ransomware

In late November 2020, the Huntsville City Schools district in Alabama experienced a ransomware attack. The district was forced to cancel classes for its 24,000 students and urged students and parents to avoid using laptops and other school-issued devices. Compromised data reportedly included Personally Identifiable Information (PII) such as state student identification numbers, parent email addresses, employees' Social Security numbers, and information from contractors who worked with the district between 2010 and 2020. The district worked with outside cybersecurity experts to recover backup files, install and implement additional cybersecurity software, and issue new devices to faculty and staff.[5]

Hartford City Schools Ransomware

In September 2020, Hartford City Schools in Connecticut experienced a ransomware attack on the first scheduled day of the school year. The ransomware attack forced the district to postpone opening its public schools to its 18,000 students, despite planning for a hybrid model where some students would return to school buildings. In Hartford, the school district shares technology resources with the city government, and the city had invested about $500,000 upgrading its security system in 2019. This investment helped the city successfully respond to this attack. Within two days, city employees were able to restore systems compromised in the attack and reopened schools.[6]

Video Bombing

Wyoming City Schools Video Bombing

During 2020, the Wyoming City Schools district in Ohio was the victim of at least two video bombing incidents. The Wyoming middle schools experienced two separate incidents that were reported by a district spokesperson. In one incident in July 2020, a parent information session held through a publicly available link was disrupted by an unauthorized individual who appeared on-screen unclothed and shouting profanities. In the second incident, an unauthorized individual interrupted a secured class meeting with students, but the district has not released details regarding the content

[4] Costantino, A. (2020). With Data Presumed unrecoverable, Baltimore County Schools scramble to recover from cyber-attack. Baltimore Brew (December 18, 2020). Retrieved March 9, 2021 from https://baltimorebrew.com/2020/12/18/with-data-presumed-unrecoverable-baltimore-county-schools-scramble-to-recover-from-cyber-attack/; Goud, N. (2020). Baltimore County Public Schools Hit by Ransomware Attack. *Cybersecurity Insiders* (no date). Retrieved March 9, 2021 from https://www.cybersecurity-insiders.com/baltimore-county-public-schools-hit-by-ransomware-attack/

[5] Kobialka, D. (2020). Huntsville, Alabama School District Ransomware Attack Recovery Update. *MSPP Alert* (December 7, 2020). Retrieved March 9, 2020 from https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/huntsville-alabama-schools-system/; WAFF Digital Staff (2020). Huntsville City Schools Issues Cyberattack Update. (December 21, 2020). Retrieved March 9, 2020 from https://www.waff.com/2020/12/21/huntsville-city-schools-issues-cyber-attack-update-monday/

[6] Gold, D. (2020). First Pandemic, Now Ransomware: Attack Forces Hartford to Postpone School. New York Times (September 8, 2020). Retrieved March 9, 2021 from https://www.nytimes.com/2020/09/08/nyregion/hartford-schools-ransomware.html

that may have been shared by the unauthorized individual. In response to these incidents, Wyoming City Schools have improved their video conferencing security settings and standards.[7]

Phishing

Manor Independent School District Phishing Attack

In January 2020, the Manor Independent School District in Manor, Texas, was the victim of a fraudulent email campaign. The district was targeted with phishing emails from cybercriminals beginning in November 2019 and reports indicate that at least three fraudulent transactions resulted from the email campaign. These transactions totaled $2.3 million, which the district is seeking to recover through a law enforcement investigation. To date, the cybercriminals involved in the phishing scheme have not been identified, and Manor Independent School District has had to bear the entire cost of the fraudulent transactions.[8]

[7] Mitchell, Madeline. 'We will not be doing that again.' Local schools report 'Zoom-bombings,' increase security measures. *Cincinnati Enquirer* (September 2, 2020). Retrieved March 9, 2021, https://www.cincinnati.com/story/news/2020/09/02/zoom-bombing-local-schools-prompt-investigations/5687217002/

[8] Osborne, Charlie (2020). Texas school district falls for email scam, hands over $2.3 million. *ZDNet,* (January 13, 2020). Retrieved March 9, 2021, https://www.zdnet.com/article/texas-school-district-falls-for-scam-email-hands-over-2-3-million/.

Appendix D: Attacks and Facts

Distributed Denial of Service

Distributed Denial of Service (DDoS) attacks overload bandwidth and connection limits of hosts or networking equipment, specifically through a network of computers making excessive connection requests. DDoS attacks unfold in stages. First, a malicious actor infects a computer with malware that spreads across a network. This infected computer is known as the "master" because it controls any subsequent computers that become infected. The other infected computers carry out the actual attack and are known as "daemons." The attack begins when the master computer sends a command to the daemons, which includes the address of the target. Large numbers of data packets are sent to this address, where extremely high volumes (floods) of data slow down web server performance and prevent acceptance of legitimate network traffic. The cost of a DDoS attack can pose sever loss of revenue or reputation to the victim.

More information on DDoS attack possibilities within each layer of the Open Systems Interconnection (OSI) Model, as well as traffic types and mitigation strategies, can be found in the resource list below.

Additional Resources

- Understanding Denial-of-Service Attacks (https://www.us-cert.gov/ncas/tips/ST04-015)
- DDoS Quick Guide (https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf)
- Guide to DDoS Attacks (https://www.cisecurity.org/wp-content/uploads/2017/03/Guide-to-DDoS-Attacks-November-2017.pdf)

Social Engineering

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering–the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing, i.e., email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for breaching networks, evading intrusion detection systems without leaving a log trail, and is completely operating system platform dependent. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, to include training personnel to be cautious of suspicious emails, know where to forward them and keeping software and systems up to date.

Additional Resources

- Avoiding Social Engineering and Phishing Attacks (https://www.us-cert.gov/ncas/tips/ST04-014)
- The Most Common Social Engineering Attacks (https://resources.infosecinstitute.com/common-social-engineering-attacks/)

Ransomware

Ransomware is a type of malware that denies access to victims' data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency, so the victim can receive a decryption key. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Additional Resources

- CISA Ransomware (https://www.cisa.gov/stopransomware)
- Protecting Against Ransomware (https://www.us-cert.gov/ncas/tips/ST19-001)
- Indicators Associated with WannaCry Ransomware (https://www.us-cert.gov/ncas/alerts/TA17-132A)
- Incident trends report (Ransomware) (https://www.ncsc.gov.uk/report/incident-trends-report#ansomware)

Appendix E: Doctrine and Resources

Laws

- National Cybersecurity Protection Act of 2014 (Dec 2014) https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf
- Federal Information Security Modernization Act of 2014 (Dec 2014) https://www.dhs.gov/fisma
- OMB Memorandum: M-15-01, Fiscal Year 2014-2015: Guidance on Improving Federal Information Security and Privacy Management Practices (Oct 2014) https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf

Presidential Directives

- Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017) https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
- Presidential Policy Directive-41: United States Cyber Incident Coordination (Jul 2016) https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
- Annex to Presidential Policy Directive-41: Annex to the Directive on United States Cyber Incident Coordination (Jul 2016) https://www.hsdl.org/?view&did=797545
- Presidential Policy Directive-8: National Preparedness (Mar 2011), (Updated Sep 2015) https://www.dhs.gov/presidential-policy-directive-8-national-preparedness
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Feb 2013) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013) https://www.hsdl.org/?view&did=731040

Strategies and Frameworks

- National Cyber Incident Response Plan (Dec 2016) https://www.us-cert.gov/ncirp
- National Cyber Strategy of the United States of America (Sep 2018) https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
- U.S Department of Homeland Security Cybersecurity Strategy (May 2018) https://www.hsdl.org/?view&did=810462
- Framework for Improving Critical Infrastructure Cybersecurity (Apr 2018) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- National Protection Framework, Second Edition (Jun 2016) https://www.fema.gov/media-library-data/1466017309052-85051ed62fe595d4ad026edf4d85541e/National_Protection_Framework2nd.pdf
- Office of Management and Budget (OMB) Memorandum: M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (Oct 2015) http://www.thecre.com/forum4/wp-content/uploads/2015/11/OMB-Cybersecurity-Implementation-Plan.pdf

Key Points of Contact

- Cybersecurity and Infrastructure Security Agency (CISA) (contact: central@cisa.dhs.gov)
- Federal Bureau of Investigation (FBI)
  - Field Office Cyber Task Forces (contact: https://www.fbi.gov/contact-us/field-offices)
  - Internet Crime Complain Center (IC3) (contact: http://www.ic3.gov)
- National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; (855) 292-3937)
- United States Secret Service Field Offices and Electronic Crimes Task Force (ECTFs) (contact: https://www.secretservice.gov/contact/field-offices/)

Other Available Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; (518) 266-3460)
- Cybersecurity and the States (National Association of State Chief Information Officers [NASCIO]) (http://www.nascio.org/Advocacy/Cybersecurity)
- National Governors Association (NGA) (https://www.nga.org/)
- DHS Cybersecurity Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- InfraGard (https://www.infragard.org/)
- Internet Security Alliance (http://www.isalliance.org/)
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (https://www.isao.org/information-sharing-groups/)
- International Association of Certified ISAOs (http://www.certifiedisao.org; contact: operations@certifiedisao.org)
- National Council of ISACs (https://www.nationalisacs.org/)

References Cited

Ari Odzer, T. P. (2020, 3 September). *Student Arrested in Connection With Cyberattacks on Miami-Dade Public Schools*. Retrieved 2021, from NBC Miami: https://www.nbcmiami.com/news/local/student-arrested-in-connection-with-cyberattacks-on-miami-dade-public-schools/2287613/

Bonner, Michael (2021, 5 February). *Winthrop Public Schools, town offices targeted in cyber-attack which prevented access to Google Classroom, email, video conferencing*. Retrieved 2021, from MassLive: https://www.masslive.com/boston/2021/02/winthrop-public-schools-town-offices-targeted-in-cyber-attack-which-prevented-access-to-google-classroom-email-video-conferencing.html

Costantino, A. (2020, 18 December). *With Data Presumed unrecoverable, Baltimore County Schools scramble to recover from cyber-attack.* Retrieved 2021, from the Baltimore Brew: https://baltimorebrew.com/2020/12/18/with-data-presumed-unrecoverable-baltimore-county-schools-scramble-to-recover-from-cyber-attack/

Gold, D. (2020, 8 September). *First Pandemic, Now Ransomware: Attack Forces Hartford to Postpone School.* Retrieved 2021 from The New York Times: https://www.nytimes.com/2020/09/08/nyregion/hartford-schools-ransomware.html

Goud, N. (2020). *Baltimore County Public Schools Hit by Ransomware Attack*. Retrieved 2021, from Cybersecurity Insiders: https://www.cybersecurity-insiders.com/baltimore-county-public-schools-hit-by-ransomware-attack/

Kobialka, D. (2020, 7 December). *Huntsville, Alabama School District Ransomware Attack Recovery Update.* Retrieved 2021, from MSPP Alert: https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/huntsville-alabama-schools-system/

Mitchell, Madeline (2020, 2 September). *'We will not be doing that again.' Local schools report 'Zoom-bombings,' increase security measures.* Retrieved 2021, from the Cincinnati Inquirer: https://www.cincinnati.com/story/news/2020/09/02/zoom-bombing-local-schools-prompt-investigations/5687217002/

Osborne, Charlie (2020, 13 January). *Texas school district falls for email scam, hands over $2.3 million.* Retrieved 2021, from ZDNet: https://www.zdnet.com/article/texas-school-district-falls-for-scam-email-hands-over-2-3-million/.

Traffic Light Protocol (TLP) Definitions and Usage. Retrieved 2021, from https://www.cisa.gov/tlp.

Wadhwani, S. (2020, 3 September). *DDoS Attacks Plague Miami-Dade County Public Schools*. Retrieved 2021, from https://www.toolbox.com/security/network-security/news/ddos-attacks-plague-miami-dade-county-public-schools/.

WAFF Digital Staff (2020, 21 December). *Huntsville City Schools Issues Cyberattack Update*. Retrieved 2021, from https://www.waff.com/2020/12/21/huntsville-city-schools-issues-cyber-attack-update-monday/