READINESS AND EMERGENCY MANAGEMENT FOR SCHOOLS
REMS
TECHNICAL ASSISTANCE CENTER

Cybersecurity Tabletop Exercise

FOR MORE INFORMATION

(855) 781-REMS (7367) ✉ info@remstacenter.org @remstacenter https://rems.ed.gov

Cybersecurity Tabletop Exercise Participant Guide

For information on how to lead the tabletop exercise, see the accompanying document "Emergency Exercises Training Package Instructions" within the Emergency Exercises Package.

In this tabletop exercise, you should imagine that you are a member of your school's emergency planning team and that you have access to only the resources and systems you currently have in place. You will discuss your response to a hypothetical cybersecurity incident, specifically a data breach that occurs as a result of malware.

A scenario will first be presented to you and then be followed by individual questions. After each question is asked, you should pause and discuss it with your group. Additional information on how the scenario unfolds, called injects, and questions are then posed on how the school would respond.

Scenario

You work in a school district with a centralized information technology (IT) system, wherein most IT services are managed at the district level. The district also operates a Student Information System (SIS), where teachers from all schools throughout the district input student attendance, grade, and assessment data.

At 5:30 p.m. on a Friday in April, a teacher at your school puts in a help desk ticket with your district's IT department, stating that their school computer has been running more slowly than usual and that this past week, when they tried entering attendance data and grades, it was freezing and needed to be restarted often. The district IT manager makes a note to inspect the computer on Monday morning and leaves for the weekend.

On Saturday afternoon, several worried parents call your school and leave messages with staff members, stating that their child's grades have been made publicly available on the school's Website. After nearly an hour of frantic phone calls, the school administrator is reached, who navigates to the Website and finds that the pages look different — dozens of student grades have been posted to the Website's main homepage, and the rest of the site's pages are no longer functioning. Your school administrator requests to convene your school's emergency response team, of which you are a member, to decide next steps. Members of the team travel to the school to meet.

Discussion Questions

Now, please answer the following questions. As you answer them, have a volunteer take notes to help later with the exercise debrief.

1. What would be your team's first steps? Do you have existing protocols for what to do in this type of situation, such as in the Cyber Annex to your school emergency operations plan (EOP)?
2. With whom would you need to communicate, such as your district's IT department, district administration, or school administration? How would you do that, particularly on a Saturday? Do you have established protocols in the Communications and Warning Annex?
3. What statement would be provided in response to parents' and community members' continued inquiries?

Now that the team has discussed these questions, you'll hear how the scenario hypothetically unfolds with Inject #1.

Inject #1

Your school administrator decides to contact your district's IT department and the district superintendent. The district superintendent navigates to the Websites of other schools in the district and finds that student grades have also been posted to two other schools' Websites. School phone lines around the district are quickly becoming flooded with calls from the community about the incident, as now hundreds of students' names and grades have been made public. The district IT team begins its investigation on Saturday evening, looking into district system logs. They find that the SIS was accessed late the night before, and a user was able to export classroom-level data, including student records, from several schools in the district. The district administrator relays to your team that the investigation is ongoing, but that all the schools' Websites in the district will be offline for the foreseeable future.

Your school's Website is the main hub for communicating with the school community, and multiple news and event updates were scheduled to be posted to the Website on Monday morning, including the location and hours of a vaccine clinic and a food pantry event that week. Additionally, the Website hosts an online form where families have been registering their students for the upcoming summer program. The Website also contains a built-in feature for users to translate information into other languages commonly spoken within your school community.

Discussion Questions

Now, answer the following questions:

1. Would you need to update anyone about what is happening with the investigation? If so, whom would you update and how often? Again, are those actions described in the Communications and Warning Annex?
2. How would you communicate updates to the school community regarding important upcoming events and services if the Website will be down for an unknown length of time? Do you have protocols for what to do in this situation, such as established secondary channels of communication? Are all students' emergency contact information available and up to date? How would you ensure translation services to communicate with caregivers and community members who speak other languages?
3. What other events, services, or activities rely on the school's Web presence? Are there any other Web forms or connected applications that school community members would need to access while the Website is offline? How would your school manage these processes? Do you have any established protocols for what to do, such as in the Continuity of Operations Annex to your EOP?
4. Are there any other groups or organizations that rely on the school's Website to communicate with the school community that would need to be notified?
5. School district participants: Whom would you contact during your investigation and for what purpose? Would you contact the local law enforcement agency, legal counsel, or another entity? What information would you share?

Read on to learn about how the scenario hypothetically unfolds with Inject #2.

Inject #2

Your team makes short-term response and communications plans and agrees to reconvene on Sunday when the district has more information from the investigation. On Sunday morning, your team reconvenes, and your school administrator receives a call from the district superintendent, who provides an update based on the district's investigation — the user who signed into the SIS and exported student data used the log-in credentials of a teacher at your school. The district IT manager notes that the teacher named in the investigation is the same one who put in the help desk ticket for computer support. The district superintendent states that the district team is still uncovering the extent of the data breach, the affected students, and the impacted systems, but requests that your school contact the teacher for further questioning and collect the teacher's computer so it can be scanned for viruses and malware. Additionally, the district superintendent alerts your team that no one should access the SIS until all log-in credentials can be reset. To complicate matters, social media posts are now circulating with speculations about the origin and impact of the incident, and the local news station has contacted your school for a statement.

Discussion Questions

Now, answer the following questions:

1. How have your concerns and reactions changed with this updated information? Is there anyone else you need to contact or update?
2. Does your school have a Public Information Officer or designated faculty member to handle situations involving the media and press? If you have not done so already, draft your school's formal statement on the incident.
3. Given that it is a Sunday, who would continue to respond to phone calls and emails and help to combat misinformation online? How often would you provide updates regarding the incident? How would these communications be translated into other languages to ensure that the whole school community is well informed?
4. School district participants: After consulting legal counsel, would you notify the parents and families of students whose names and grades have been released? How do Federal, state, and local laws require you to proceed with a data breach?

Now, we're moving on to Inject #3.

Inject #3

On Monday morning, the district IT manager conducts a scan of the teacher's computer, which reveals that a malicious keylogger malware is installed and operating in the background, causing the computer's slow functioning. This malware has been surreptitiously recording all the teacher's keystrokes and sending the logs to a remote system. Records indicate that the teacher's log-in credentials to the SIS were recorded, sent to another computer, and later used to access the SIS after school hours. When questioned, the teacher mentions having opened an attachment earlier that week from an email that claimed to have been an important software update. This cyber threat the teacher fell victim to is known as phishing. The email was identified, and it was confirmed that the attachment initiated the malware download that infected the teacher's computer.

Later that day, your school's administrator receives an email from the district superintendent with the names of all the students from your school who were impacted by the data breach and instructions for notifying their families. The district also alerts your school that the Website issues will be handled at the district level and are still being remediated, but that the Website should be back online by Wednesday. Additionally, temporary usernames and passwords to the SIS will be issued to all school staff, who will need to create new log-in credentials as soon as possible. Lastly, the email states that more information on new multifactor authentication protocols for accessing the SIS will be forthcoming, as well as updated defense mechanisms for all school-issued devices and new training requirements for all schools in the district.

Discussion Questions

Again, answer the following questions:

1. What services could you provide to the affected families, such as a point of contact for further questions? How would you rebuild trust with the school community in the security of your cyber infrastructure?
2. Does your school have processes and procedures to ensure a successful recovery from a cybersecurity incident, such as in the Recovery Annex to your school EOP?
3. What further cybersecurity and/or cyber safety training might school staff need? How and how often would these trainings be delivered?
4. School district participants:
   - Does your district have the resources to effectively clean the infected computer (hardware, software, labor, etc.) from the malware and to issue the teacher a new computer in the meantime? Would any additional support, expertise, or equipment be needed?
   - What processes would your team put in place to ensure stronger cybersecurity controls for your IT systems in the future? How would the district safeguard students' personally identifiable information after this incident?

This concludes the exercise.

Conclusion

An exercise debrief — called a "hot wash" — should now be conducted, and an after-action report developed, which identifies and documents gaps, shortfalls, and lessons learned. You should consider

1. What did the exercise demonstrate about how the school or school district would respond to this type of emergency event?
2. What went well in the exercise?
3. What lessons were learned?
4. What gaps in the school's or school district's EOP, including annexes, were identified?
5. How will the EOP and annexes be revised, if needed?
6. Who will be responsible for making these revisions?
7. By when will these revisions be made?

Resources on Preparing for Cyber Threats That Impact K-12 Schools

Cyber Annex Development

Cybersecurity Considerations for K-12 Schools and School Districts, Fact Sheet (REMS TA Center). Shares useful information about key cybersecurity considerations for schools and school districts.

Cyber Safety Considerations for K-12 Schools and School Districts, Fact Sheet (REMS TA Center). Describes the many cyber threats facing schools and school districts, and provides preparedness actions to take before, during, and after a cyber threat.

Cybersecurity Considerations for K-12 Schools and School Districts, Online Course (REMS TA Center). Helps users understand the cyber threats facing K-12 schools and districts; how schools and school districts can prepare for, respond to, and recover from cyber threats; and how to integrate cybersecurity into an emergency operations plan (EOP).

Integrating Cybersecurity With Emergency Operations Plans (EOPs) for K-12 Schools, Webinar (REMS TA Center). Focuses on the importance of cybersecurity and network protection at schools and school districts, and details steps for integrating cybersecurity into EOPs.

Creating, Revising, and Enhancing Emergency Operations Plans to Support Cyber Safety, Podcast (REMS TA Center). Features a two-part discussion on cyber safety in school settings, detailing examples of cyber threats, digital citizenship programs, and strategies for education agencies to build their preparedness capacity against cyber threats.

Addressing Adversarial and Human-Caused Threats That May Impact Students, Staff, and Visitors, Web Page (REMS TA Center). Contains Federal guidance and resources on addressing human-caused threats, and includes a filter for cybersecurity and cyber safety.

Understanding the Role of Information Technology Specialists in Supporting School Safety Before, During, and After an Emergency, Webinar (REMS TA Center). Explores the role of information technology specialists in supporting school EOP development, including cybersecurity planning.

Cybersecurity Exercises

CISA Tabletop Exercises Packages, Web Page (U.S. Department of Homeland Security [DHS], Cybersecurity and Infrastructure Security Agency [CISA]). Contains a variety of customizable tabletop exercise packages, which contain exercise objectives, scenarios, discussion questions, and supplemental resources. Under the "Cybersecurity Scenarios" section, there is an exercise package specifically designed for K-12 schools.

Data Breach Response Training Kit, Downloadable Materials (U.S. Department of Education [ED], Privacy Technical Assistance Center [PTAC]). Details a simulated data breach scenario, and guides participants through developing an effective response plan.

Dual Enrollment Data Breach Scenario, Publication (ED, PTAC). Simulates a data breach scenario involving interagency student data sharing, prompting participants to navigate the incident through guiding questions and to develop a response plan.

Malicious Software Data Breach Scenario, Publication (ED, PTAC). Simulates a data breach scenario involving ransomware, and directs participants to navigate response and recovery efforts.

Cybersecurity Incident and Vulnerability Response Playbooks, Publication (DHS, CISA). Provides a standard set of operational procedures for planning and conducting cybersecurity vulnerability and incident response activities.

Tool Box, Web Page (REMS TA Center). Contains materials for planning, conducting, and evaluating emergency exercises.

Cyber Mitigation and Protection

Getting Smarter About K-12 Cybersecurity, Webinar (DHS, CISA). Explores how schools and school districts can protect their systems from cyberattacks and threats.

K-12 Cybersecurity Self Assessment, Web Page (EdTech Strategies). Helps information technology leaders at the district level assess the strength of their cybersecurity controls.

Cyber Security and Protecting Students and Staff, Community of Practice Forum (REMS TA Center). Shares a discussion on cybersecurity and protecting staff and student data.

Cyber Threats to K-12 Remote Learning Education, Fact Sheet (DHS, CISA). Describes common cyber threats to remote learning, and provides best practices for schools to implement to strengthen preparedness against cyberattacks.

Secure Video Conferencing for Schools, Web Page (DHS, CISA). Offers a downloadable tip sheet and recommendations for conducting safe video conferencing for schools.

StopRansomware.gov Website, Website (DHS, CISA). Provides resources, guidance, tools, and training opportunities for preventing, responding to, and recovering from ransomware attacks, including the comprehensive Ransomware Guide. This Website also hosts a K-12 Resources page to support education agencies in enhancing their cybersecurity controls to protect against ransomware and other cyber threats.

Protect Your Network: Strengthen Your Cybersecurity With Our Incident Response Training, Videos (DHS, CISA). Watch this series of Webinars focused on cyber incident response training for government employees and contractors in Federal, state, local, tribal, and territorial agencies.

Building Technology Infrastructure for Learning, Publication (ED, Office of Educational Technology). Use this K-12 school infrastructure guide to navigate the many decisions required to build a technology infrastructure that supports digital learning.

FERPA and Virtual Learning Related Resources, (ED, Student Privacy Policy Office). Access this publication for available resources on the Family Educational Rights and Privacy Act (FERPA) and virtual learning.

Recovery From Cyber Threats

K-12 Education Leaders' Guide to Ransomware: Prevention, Response, and Recovery, Webinar (DHS, CISA). Shares information about ransomware, and offers strategies schools can implement to strengthen preparedness against ransomware attacks.

Guide for Cybersecurity Event Recovery, Publication (U.S. Department of Commerce [DOC], National Institute of Standards and Technology [NIST]). Outlines how to improve resilience and plan for recovery against cybersecurity threats.

Creating a Culture of Cyber Preparedness

Cybersecurity for Teachers, Web Page (DHS, CISA). Visit this Web page to access K-12 cybersecurity curricula and education tools.

Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness, Publication (DHS, CISA). Explores how to build a culture of cyber readiness and develop an actionable understanding of where to start implementing organizational cybersecurity practices.

Cyber.org, Web Page (DHS, CISA). Hosts a virtual library of curricular materials to help teach K-12 students about cybersecurity and cyber safety. The Website also hosts the Cyber Safety Video Series that contains short videos and accompanying tip sheets for youth on topics such as social media safety, strong passwords, online gaming safety, and more.

NetSmartz®, Web Page (National Center for Missing and Exploited Children). Contains classroom activities and supplemental resources for teaching children and youth about cyber safety and digital citizenship.

FBI Safe Online Surfing Internet Challenge, Web Page (U.S. Federal Bureau of Investigation). Hosts an educational program to teach students in grades 3-8 about cybersecurity and cyber safety.

Kids and Socializing Online, Web Page (U.S. Federal Trade Commission). Provides parents with guidance for talking to children and youth about cyber safety, and hosts the guide Net Cetera: Chatting With Kids About Being Online for continuing these conversations. The Web page is available in Spanish, and the guide is also available in Spanish.

Protecting Kids Online, Web Page (U.S. Federal Trade Commission). Access resources on talking to kids about cybersecurity and cyber safety.

A Parent's Guide for Understanding K-12 School Data Breaches, Publication (ED, PTAC). Offers information about school data breaches to a parent or family member of a K-12 student.

General Cybersecurity and Cyber Safety

Cybersecurity, Web Page (DHS, FEMA). Provides information about cyberattacks as well as measures that individuals and organizations can prepare to take before, during, and after a cyberattack.

Cybersecurity, Web Page (DHS, CISA). Offers resources related to topics in cybersecurity and cyber safety, including ransomware, information sharing, and multifactor authentication.

Cybersecurity Framework, Web Page (DOC, NIST). Shares risk management principles and best practices to help organizations improve their cybersecurity measures.

Be Prepared for a Cyberattack, Publication (DHS, FEMA). Shares facts about cyberattacks, as well as preparedness and protective actions that individuals can take to stay safe before, during, and after a cyberattack.

Nationwide Cybersecurity Review, Web Page (Center for Internet Security, Multi-State Information Sharing and Analysis Center). Complete this no-cost, anonymous, annual self-assessment to receive organization-specific metrics to identify gaps in your current cybersecurity capabilities, develop a benchmark to gauge progress, and gain access to a repository of informative resources.