MARYLAND CENTER for SCHOOL SAFETY

Weekly Tabletop Exercises

Date:

Facilitator:

Participants:

Which part of your Emergency Plan are you reviewing:

Scenario: Your middle school has a small IT department equipped to handle everyday technology tasks. The Local Education Agency, also known as an LEA, has a centralized IT department that is responsible for handling technology issues on a grander scale. The centralized IT department manages the Student Information System, where all student information is stored. The information in this system includes things such as attendance, grades, assessment details, and some personal information.

On Monday, the middle school begins receiving phone calls and emails from parents of students stating that their child's information has been made public on the school's website. Upon further investigation, it is apparent to the IT department that when parents search the school website for their child's homeroom information and school supply list, they can see each teacher's class list, with students' names showing as a clickable link. Once you click a student's name, you can see their grades, state test scores, and the child's emergency card information. An emergency card is private, with details and personal phone numbers and addresses provided.

While your IT department is scrambling to investigate how this breach started, they review their most recent help tickets. They recall the ticket sent the previous week from your middle school teacher who was complaining about a slow computer. Further inquiry discovered that the breach might be connected to this teacher's computer.

The email appeared as though it was sent from Admin, who gave instructions requiring information updates for all staff, which could be completed by clicking the link provided.

The local news station has gotten wind of the situation, keeping your administration staff busy. With the beginning of school only a couple of days away, you are busy, to say the least! The superintendent informs you that the districtwide IT department has discovered the source of the malware, and they are taking active steps to clean the breach up, as well as work to build a stronger security network. Unfortunately, the unease this has caused in your school community is at an all-time high. Your superintendent has called an emergency meeting with the principal, and IT support staff members from every school in your district to discuss the ramifications of this breach as well as mitigation strategies.

MARYLAND CENTER for SCHOOL SAFETY

BEFORE	DESCRIBE MAJOR DETAILS ABOUT THE INCIDENT
What data has been compromised?	
Is the data breach still occurring?	
What are the IT department's next steps?	
When does the IT department outsource assistance?	

DURING	DESCRIBE MAJOR DETAILS ABOUT THE INCIDENT
What are the next action steps to be taken?	
Have you set up a defensible path?	
Does your Emergency Plan have a strategy for addressing a data breach? If so, has it ever been tested?	
Have you determined whether the data breach was accidental or malicious?	
How does this developing situation change your procedures or actions?	
With school set to begin in a couple of days, how will you disseminate	

DURING	DESCRIBE MAJOR DETAILS ABOUT THE INCIDENT
information with a downed website?	
Has any of the staff's personal information been compromised at this point?	
Who else is involved? Police? Vendors?	

AFTER-ACTION	DISCUSS IMPORTANT DETAILS ABOUT THE INCIDENT
Have you researched your legal obligation for breach notification?	
What other potential crises might we encounter as a school community?	
Have you implemented a crisis communications plan?	
What can we do to avoid future disasters?	

RESOURCES

Visit **SchoolSafety.Maryland.gov**, go to "Resources", then "Training & Exercise"

CONTACT INFO

Brittani Ayers, School Prevention and Intervention Specialist **brittani.ayers@maryland.gov**