Cybersecurity Annex Tip Sheet

Each school's building-level emergency response plan (ERP) includes functional annexes that outline action steps to respond to a variety of different emergencies. The school's building-level emergency response team (the "planning team") should ensure that each school plan documents the action steps necessary to maintain safety in response to different types of threats or hazards that may occur in the school.

School and school district computer networks and systems are increasingly the target of cyber threats including hacking of private data records and the targeting of K-12 schools for ransomware attacks. Ransomware is a particular form of computer malware in which perpetrators encrypt users' files, then demand the payment of a ransom for users to regain access to their data. New York's schools have been frequent targets of such attacks. [1,2,3]

As such, beginning in the 2021-22 school year, the ERP template that is used to collect plans from schools at the beginning of each school year includes an optional Cybersecurity Annex. A functional annex outlines critical actions and steps you will take during an emergency. The annex should include goals, objectives, and courses of action for before, during, and after the incident. Courses of action should clarify the action, who is responsible, when the action will take place, what will or can happen before and after, the resources needed, and how to consider specific populations.

To develop a Cybersecurity Annex, building-level emergency response teams should work with their information technology team and data coordinator to outline the necessary actions to take before, during, and after a cybersecurity incident. To protect networks and systems before an incident, schools and districts should consider an overall preparedness program that includes, but is not limited to, policies and programs for responsible use, storage of secure data, firewalls, and network monitoring. Members of the school community need to know to whom they should report a cybersecurity incident. Immediate actions may include (but are not limited to) disconnecting impacted devices from the network, taking the network offline, powering down devices, notifying appropriate information security staff. Once the incident has been contained, the team will need to identify what technology was impacted, what people were impacted, what caused the incident, and how to prevent future incidents from occurring. Additional actions may include notifying the Cyber Security and Infrastructure Security Agency (CISA), your local Federal Bureau of Investigation (FBI) field office, the FBI Internet Crime Complaint Center, or your local U.S. Secret Service Office. If an incident does occur, the team should also conduct a meeting after the event to document information from the event and make appropriate revisions to their plan.

---

[1] https://www.govtech.com/education/k-12/guilderland-central-schools-hit-with-malware-attack
[2] https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/ryuk-hits-rockville-centre/
[3] https://www.zdnet.com/article/texas-california-new-york-and-louisiana-missouri-lead-list-of-states-with-most-ransomware-attacks-on-schools-report/

In addition to a school or district's own information technology staff, suggested informational resources are listed below.

- Cybersecurity Considerations for K-12 Schools and School Districts and Cyber Safety Considerations for K-12 Schools and School Districts prepared by the US Department of Education's Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center.
- The Cybersecurity and Infrastructure Security Agency maintains a Stop Ransomware webpage with resources and training, including resources specific to schools, including an online webinar.
- SchoolSafety.gov is an interagency collaboration that distributes resources from the U.S. Departments of Homeland Security (DHS), Education (ED), Justice (DOJ), and Health and Human Services (HHS) to share actionable recommendations to keep school communities safe by helping schools prevent, protect, mitigate, respond to, and recover from emergency situations.