PLANNING & IMPLEMENTATION METHODS

During the pandemic, work units established continuity plans that defined which services would be prioritized as staffing became constrained. These plans provide the framework for an orderly transition from conventional to contingency standards of care and outline triggers for modifying or reducing services and activities. In the clinical laboratories, those testing that would be discontinued is defined and reviewed annually. In a national survey, 82.4% of hospitals included cybersecurity disasters in their Hazard Vulnerability Analyses (HVAs), but more than half did not have an Emergency Operations Plan in place related to cybersecurity.

Most laboratory instruments can run without network connectivity; however, all required specimen information, reconciliation of results, and communication back to providers must be managed through manual processes. Nearly all lab testing will need to be augmented by other trained lab professionals and non-lab personnel to handle the increased specimen and data management needs. Impairment of building control systems will impact air circulation and temperature, and potentially other essential utility services, which will further constrain staffing. Collaborative planning with hospital leadership will need to occur to direct testing capacity to the highest priority patient care needs.

CONCLUSIONS

As part of emergency preparedness/continual readiness, Mayo Clinic has required a cyberattack plan for its business units. Through the process of planning a response for a cyberattack, there are key items that need to be considered in an affective response - patient care continuity, a triage and prioritization process, defining network dependency, and outlining communication pathways.