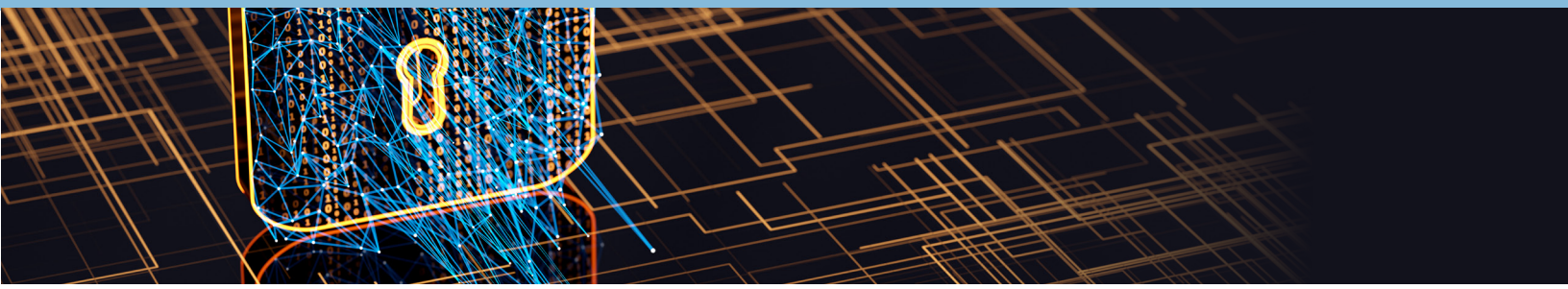
Health-ISAC Preparedness & Resiliency Exercise Series After-Action Report 2022

This exercise series generously sponsored by:

ordr | MedSec | proofpoint

Health-ISAC™
Collaborating for Resilience in Healthcare

health-isac.org



Executive Summary

Health-ISAC (Health Information Sharing and Analysis Center) held several exercises in 2022 as part of the Health-ISAC Preparedness & Resiliency Exercise Series. The exercises included participants from various Healthcare and Public Health (HPH) sector stakeholders.

The exercises were held in-person at locations throughout the United States and included an evolving ransomware scenario. Participants shared best practices, resources, real-life experiences, and recommendations for continuous improvement. The full version of the After-Action Report was made available to Health-ISAC members.

The exercise series explored challenges and opportunities facing the resiliency of the healthcare sector due to the increasingly interconnected nature of cyber and physical systems and interdependencies. The exercises also addressed the increased potential for attacks impacting both physical and cybersecurity operations.

Throughout the series, observations addressed the importance of effective collaboration and explored a number of opportunities that may further enhance security and resiliency across the healthcare community. The observations and learnings from the exercises were consolidated into the following eight category summaries. Health-ISAC encourages health IT and cyber security professionals consider these lessons learned for continuous improvement in their own organizations. A short summary of the information discussed is included for the eight categories.

- **Malware Detection:** Vulnerabilities preventing malware detection include engineering factors such as misconfiguration of the network, improperly managed or unmanaged endpoints, application vulnerability due to insufficient logging, detection, and monitoring and active response activities.
- **Communications:** Participants noted they would contact Health-ISAC to help prevent propagation by sharing appropriate information. Secondary and tertiary communications are a necessary precaution for cyber incidents. The importance of internal and external messaging to help provide timely information to personnel and avoid misunderstandings of ongoing events was noted.
- **Employee Cybersecurity Training:** The importance of employee cyber training was mentioned as the best opportunity to minimize human error. The frequency of staff training must consider the ever evolving and expanding threat landscape. Consider making this training engaging, fun, and held on a regular basis.
- **Crisis Management Team:** Organizations consider response teams as expandable and collapsible as appropriated for each response. Third party technical consultants could be engaged to help remediate where applicable. The incident commander runs the response and makes appropriate decisions. Consider rotating incident commanders during exercises to enable appropriate training for personnel.

- **IT / OT Facilities and Emergency Management Integration:** IT and OT usually have their own risk management system operating differently from facilities. They use a different lexicon and have differing structures and priorities.
- **Ransom Payment Decisions:** Total operational and reputational cost to recover versus cost of paying the ransom should be considered when deciding whether to pay a ransom. Prior to an incident, consider identifying critical areas that would cause the most disruption if attacked.
- **Future Cyber Incident Preventative Measures:** Robust segmentation and monitoring were suggested as best practices. The importance of limiting privileged access was noted. An investment in education and training has cost effective rewards by making the human component the strongest link. Organizations should exercise plans and procedures on a regular basis.
- **Miscellaneous:** The understanding of interconnections of servers and systems is enhanced by the institutional knowledge of existing employees—this provides value in asset management and understanding of infrastructure path. Some difficulties to segmenting include funding, interoperability, asset management, legacy issues, and staff training capability. The threat landscape and organization structure are ever-changing. Review and exercise incident response plans on a regular basis to discover gaps and ensure continuous improvement opportunities.

Feedback and suggestions on this document are encouraged and welcome or for more information about Health-ISAC

Please email **contact@h-isac.org**