2024 Health-ISAC ASHER Workshop Series After Action Report

Exercise Conducted March 27, April 16, and May 20, 2024

TLP: WHITE This report may be shared without restriction. For Health-ISAC Members be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Health-ISAC™ SHARING SINCE 2010 Collaborating for Resilience in Healthcare

health-isac.org

Executive Summary

The Active Shooter / Hostile Events (ASHER) Preparedness Workshop Series for Health Sector Facilities aimed to explore the interconnected nature of cybersecurity and physical security threats, enhance incident response coordination, identify vulnerabilities in security protocols, and foster a culture of vigilance within the health sector. Participants engaged in scenario-based discussions and key questions to enhance their threat awareness, communication strategies, and preparedness for addressing complex security challenges.

The ASHER Preparedness Workshop Series included three workshop events:
Part I: Virtual – Initial Response and Actions
Part II: Virtual – Crime Scene Management and Recovery
Part III: In-Person – Responding to a Cyber and Physical Attack on a Healthcare Facility’s IT Department

The overarching objective of these workshops was to utilize a hostile events scenario to provide participants an opportunity to interact with one another and discuss issues, concerns, best practices and other salient points that are unique to the cyber and physical security and preparedness of healthcare facilities during coordination and response to an ASHER.

The first two virtual workshops highlighted the importance of tailoring scenarios to the audience for optimal engagement and effectiveness. While the virtual workshops with scenarios tailored for physical security professionals faced challenges due to the predominantly IT and cybersecurity professional attendees, the in-person workshop took a more effective approach by shifting the scenario to an insider threat in the IT department.

This adjustment enabled all participants to actively engage and contributed significantly to the workshop's success. Moving forward, it is evident that understanding the audience composition and aligning scenarios accordingly is key to fostering meaningful participation and maximizing the impact of such critical training sessions. This experience underscores the critical role of scenario alignment with the audience in delivering impactful and fruitful training sessions in active shooter preparedness.

The first virtual workshop delved into scenario vignettes emphasizing initial response and actions, while the second workshop delved into crime scene management strategies. The virtual workshops featured scenario vignettes set in diverse healthcare settings, including a hospital, a medical device manufacturer, and a pharmaceutical company. However, it was the in-person workshop that stood out by reimagining the scenario to center on an insider threat within the IT department, a decision that led to heightened engagement and success among all participants.

Exercise Overview

Exercise Name	Part I: Active Shooter / Hostile Events (ASHER) Preparedness Virtual Workshop for Health Services – Initial Response and Actions Workshop Part II: Active Shooter / Hostile Events (ASHER) Preparedness Virtual Workshop for Health Services – Crime Scene Management and Recovery WorkshopPart III: Active Shooter / Hostile Events (ASHER) Preparedness In-Person Workshop for Health Services – Responding to a Cyber and Physical Attack on a Healthcare Facility's IT Department
Exercise Date	March 27, April 16, and May 20, 2024
Scope	The discussion-based workshops engaged participants in facilitated discussions to exchange ideas and capture processes used by Health-ISAC members.
Objectives	Utilize a hostile events scenario to provide participants an opportunity to interact with one another and discuss issues, concerns, best practices and other salient points that are unique to the cyber and physical security and preparedness of Healthcare facilities during coordination and response to an ASHER.
Scenario	Part I and II: Five vignettes focusing on active shooter scenarios were presented to participants. Vignette topics ranged from hospital to pharmaceutical manufacturer active shooter attacks and resulting impacts, giving attendees the opportunity to work through their processes and discover gaps within their organizations.Part III: Insider cyber and hostile intruder threat within a healthcare facility's IT department.
Exercise Participants	Representatives from the Health-ISAC leadership and members participated in the exercise.
Points of Contact	Jon Crosson, Director, Health Sector Resilience, Health-ISAC, EXCON@h-isac.org Geoff Mann, Physical Threat Analyst, Health-ISAC, TOC@h-isac.org

Scenario Summary

The Part I Virtual Workshop scenario delved into initial response and actions, while the Part II Virtual Workshop delved into crime scene management strategies. Both virtual workshops featured active shooter scenario vignettes set in diverse healthcare settings, including a hospital, a medical device manufacturer, and a pharmaceutical company. However, it was the in-person workshop that stood out by reimagining the scenario to center on an insider threat within the IT department, a decision that led to heightened engagement and success among all participants. Part III In-Person Workshop Scenario: Amidst the routine workday at a bustling hospital, tensions rose within the IT department due to a disgruntled employee engaging in unauthorized access attempts and data breaches. As suspicions mount and erratic behavior escalates, the employee launches a violent attack within the workplace, targeting colleagues and causing chaos. The incident presented challenges for the IT team, cyber and physical security experts, and hospital staff to respond effectively to mitigate the impact on critical IT infrastructure, safeguard employees, and ensure continuity of healthcare operations.

It is important to emphasize the critical role of identifying key issues, engaging in meaningful discussions, and formulating actionable recommendations based on the collective insights and experiences of the diverse audience from various backgrounds and different health services. By acknowledging and addressing the challenges and opportunities that emerged during the event, we created a platform for open dialogue, knowledge sharing, and collaboration among participants.

The discussions within this section aim to not only analyze the identified issues but also explore different perspectives and potential solutions shared by participants. By incorporating a range of strengths and best practices, we recognize that what may have been a challenge for one organization could offer an opportunity for learning and improvement for others.

This collaborative approach allows for the sharing of successful strategies and lessons learned among participants, bridging the gap between diverse perspectives and fostering continuous improvement and knowledge exchange across different organizations. By leveraging the collective expertise and experiences of the participants, we can identify valuable recommendations and best practices that can benefit all stakeholders involved.

Issue 1: Lack of Robust Communication Protocols

Discussion: Participants identified a lack of robust communication protocols between IT and physical security teams during an active assailant incident, potentially leading to response coordination delays.

Recommendation: Establish clear communication channels involving cyber security staff in response plans and conduct regular exercises to practice communication and coordination.

Strengths and Best Practices: Designate a communication coordinator within the incident command structure to oversee information dissemination and ensure effective communication.

Issue 2: Inadequate Training and Drills

Discussion: Participants noted a need for comprehensive training and drills to respond effectively to active assailant incidents, highlighting gaps in existing training programs. Participants also engaged in discussions on the importance of enhancing training procedures to minimize panic during active shooter scenarios.

Recommendation: Conduct regular training sessions, joint exercises, and provide access to specialized training resources for all staff members. Tailor training programs for different staff roles, along with ethical considerations for healthcare providers in crisis situations. Noteworthy initiatives such as "run, hide, fight" and the advocacy for annual mandatory training were actively discussed.

Strengths and Best Practices: Implement scenario-based training, virtual simulations, and interactive learning tools to engage participants and improve response readiness.

Issue 3: Mental Health Support and Employee Well-Being

Discussion: Concerns were raised regarding mental health support and stress management within high-pressure departments, emphasizing the need for enhanced employee assistance programs.

Recommendation: Invest in comprehensive employee support programs, encourage regular check-ins by supervisors, and provide training on recognizing signs of stress and mental health issues.

Strengths and Best Practices: Establish a proactive mental health initiative, offer confidential counseling services, and provide stress management workshops to promote employee well-being.

Issue 4: Lack of Comprehensive Documentation

Discussion: The workshop highlighted a significant issue regarding the lack of comprehensive documentation within organizations participating in emergency preparedness, particularly concerning training procedures and preparedness plans. The absence of clear documentation raised concerns about accountability and knowledge sharing during critical incidents.

Recommendation: To address the identified issue, it is recommended that organizations prioritize the thorough documentation of all training sessions and preparedness plans. Ensuring easy accessibility of these documents to all staff members and conducting regular audits to identify gaps or areas for improvement were highlighted as essential steps.

Strengths and Best Practices: Establish a centralized and easily accessible documentation repository: Create a centralized system or platform where all training procedures, preparedness plans, and related documents can be stored and accessed by all staff members. Implement version control to track updates and revisions to documentation and establish clear protocols for maintaining and updating the repository regularly. This centralized approach can improve accountability, knowledge sharing, and overall preparedness within an organization.

Issue 5: Reputation Management

Discussion: Participants expressed concerns about potential long-term impacts on reputation following critical incidents at healthcare or pharmaceutical facilities. The workshop highlighted the importance of effective reputation management strategies post-incident. Long-term reputation recovery discussions focused on proactive strategies to rebuild trust and restore reputation post-incident. Effective communication with stakeholders and coordinated outreach efforts were emphasized as essential components in the long-term recovery process.

Recommendations: Reputation Restoration Strategies: Organizations are recommended to implement measures to rebuild trust and restore reputation post-incident. Effective communication strategies, stakeholder engagement, and community outreach efforts should be prioritized in reputation management initiatives.

Strengths and Best Practices: Communication and Community Engagement: utilizing social media and media outlets for accurate and timely communication during and after an incident to foster community solidarity and customer trust was identified as a best practice. Establishing streamlined communication channels and outreach programs to engage affected individuals, promote healing, and facilitate long-term recovery were emphasized for effective reputation management.

Overall, Strength and Best Practice: Collaboration with Law Enforcement. Establishing strong communication channels and coordination strategies with law enforcement and emergency responders before a crisis occurs was deemed crucial by all participants for a swift and effective response. Building relationships with local authorities through joint trainings or events to familiarize responders with healthcare facilities was identified as a best practice for improved emergency response capabilities.

Participant Feedback

It is important to highlight a significant improvement in the feedback collection process for this event compared to past training and exercise events. In the past, there was a challenge in obtaining feedback from participants due to the use of Word or PDF forms that required participants to complete and either email or handwrite their responses.

This method often resulted in no response, delays or incomplete feedback submissions

For this event, a different approach was implemented by utilizing Microsoft Office Online Forms and a QR code for feedback collection. This innovative method enabled us to receive immediate feedback from all participants, overcoming the barriers faced with the previous feedback collection process. By leveraging technology and streamlining the feedback submission process, we were able to gather comprehensive and timely feedback from all participants, enhancing the effectiveness of the evaluation phase of the event.

Participants who took part in the in-person workshop, shared their insights and evaluations using the new feedback mechanism. The responses reflected a range of ratings from "Excellent" to "Good" across different aspects of the workshop, such as content quality, organization, and overall participant engagement. Participants particularly highlighted the value of the experience-sharing sessions, the eye-opening discussions facilitated by diverse perspectives, and the collaborative opportunities presented during the event.

One common theme among the feedback is the appreciation for the comprehensive coverage of topics related to physical security, cyber security, incident recovery, and prevention/mitigation of information security risks. Participants found the event beneficial in helping them visualize and address common issues across different organizations, thus enhancing their understanding and preparedness in their respective fields.

Suggestions for improvement for future workshops included incorporating more detailed scenarios to stimulate deeper discussions and yield more insightful outcomes. Participants also expressed interest in having more use case videos, increased visibility of the event to enhance attendance, and the provision of reference materials for further study and exploration.

Overall, the feedback underscores the positive impact of the workshop in fostering knowledge-sharing, collaboration, and skill development among the participants. The constructive suggestions offered aim to enhance the overall experience and maximize the learning potential for future iterations of similar events.

Conclusion

The ASHER Preparedness Workshops identified significant strengths, best practices and critical areas for improvement in response coordination, communication protocols, staff training, and mental health support. By implementing the recommendations and best practices, organizations can enhance their preparedness for security challenges within healthcare settings and prioritize the safety and well being of all employees, clients, patients and stakeholders.

Appendix A: Acronyms

AAR	After Action Report
AI	Artificial Intelligence
ASHER	Active Shooter / Hostile Event Response
BCP	Business Continuity Plan
CARF	COVID-19 Additional Relief Fund
CEO	Chief Executive Officer
CMS	Centers for Medicare and Medicaid Services
DHS	Department of Homeland Security
EAP	Employee Assistance Program
ED	Executive Director
EMR	Electronic Medical Record
EMS	Emergency Medical Services
ER	Emergency Room
FBI	Federal Bureau of Investigations
FDA	Food and Drug Administration
GxP	Good Practice Guidelines and Regulations
HICS	Hospital Incident Command System
HR	Human Resources
ICU	Intensive Care Unit
IR	Incident Response
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MR	Medical Record
NICU	Neonatal Intensive Care Unit
OSHA	Occupational Safety and Health Administration
PIO	Public Information Officer
PR	Public Relations
R&D	Research and Development
SWAT	Special Weapons and Tactics