New York City Long-Term Care Cybersecurity Tabletop Exercise

After-Action Report/Improvement Plan

June 1, 2022

The After-Action Report/Improvement Plan aligns exercise objectives with preparedness doctrine to include the National Preparedness Goal and related frameworks and guidance. Exercise information required for preparedness reporting and trend analysis is included. Users are encouraged to add additional sections as needed to support their own organizational needs.

CONTENTS

EXERCISE OVERVIEW

Exercise Name	NYC Long-Term Care Cybersecurity Tabletop Exercise (TTX)
Exercise Dates, Times, and Locations	Three identical sessions were held on: • April 26, 2022: 9:00 a.m. to 12:00 noon • April 26, 2022: 1:00 p.m. to 4:00 p.m. • April 27, 2022: 9:00 a.m. to 12:00 noon All sessions were conducted virtually through Zoom.
Scope	A three-hour facilitated, discussion-based TTX was conducted three times over two days. Participants in each session were presented with two vignettes for discussion.
Purpose	To examine the coordination, collaboration, information sharing, mitigation, and response capabilities of New York City nursing homes and adult care facilities' cyber incident response plans in managing significant cyber incidents. Each session included scenarios involving software as a service, data exfiltration, ransomware, and electronic medical records (EMRs).
Core Capabilities	Identify, Protect, Detect, Respond, Recover
Objectives	1 Examine the plans and abilities of New York City long-term care facilities to respond to a significant cyber incident. 2 Evaluate the ability of New York City long-term care facilities to gather and disseminate essential elements of information during a significant cyber incident. 3 Explore processes for requesting incident response resources. 4 Explore New York City long-term care facilities' processes for internal and external messaging during a cyber incident. 5 Discuss members' plans, processes, and procedures for recovering from a significant cyber incident.
Threat or Hazard	Cybersecurity incident affecting New York City long-term care facilities.
Scenario	Vignette 1: A distributed denial of service attack and data exfiltration incident impacting patient health information and personally identifiable information. Vignette 2: A compromise to participants' EMR vendor(s) that resulted in data manipulation and ransomware on their facility's systems and devices.
Grant Disclaimer	This publication was supported by the US Department of Health and Human Services (HHS) Office of the Assistant Secretary for Preparedness and Response under award number U3REP190597-03. The content is solely the responsibility of the authors and does not necessarily represent the official views of HHS.
Sponsors	Greater New York Hospital Association (GNYHA) Continuing Care with: • Greater New York Health Care Facilities Association • Southern New York Association • New York City Department of Health and Mental Hygiene (DOHMH)
Participating Organizations	See Appendix E
Points of Contact	Lisa Fenger, GNYHA (lfenger@gnyha.org) Antonia Erhabor, DOHMH (aehabor@health.nyc.gov)

EXERCISE EVALUATION AND IMPROVEMENT PLANNING

Evaluation of the exercise is based on the exercise objectives and aligned National Institute of Standards and Technology (NIST) Framework and the Hospital Preparedness Program (HPP) Capabilities – please reference Appendix D. Evaluators analyzed exercise discussion and the exercise hotwash to identify observations and related recommendations. Additionally, players were asked to complete participant feedback forms. These documents, coupled with facilitator observations and notes, were used to evaluate the exercise and compile this After-Action Report.

ANALYSIS OF EXERCISE FINDINGS

HPP Capability 1: Foundation for Health Care and Medical Readiness

- *Identify Risks and Needs*
- *Ensure Preparedness is Sustainable*
- *Train and Prepare the Health Care and Medical Workforce*

NIST Function: Identify (risk assessment)

Observation: If an EMR provider is offline for an extended period, facilities are unable to access resident records.

Analysis: Although some facilities reported that they have non-networked computers that can be used for EMRs, many did not have adequate plans for accessing and maintaining resident records if an outage occurred over several days. Facilities reported concerns that not all staff were familiar with using paper records and noted that even when access to EMR is restored, it may take significant time to input any manually created resident records. There were further concerns that having no or limited access to records could negatively impact resident care in areas such as meal and pharmacy needs.

Recommendation 1: Assess EMR downtime procedures and capabilities to determine how the organization will safely conduct resident care and confirm resident information if the EMR is offline.

Recommendation 2: Evaluate the time required for staff to input manual resident records into the EMR when the system is restored and document in the incident response and recovery planning materials. Ensure the planning materials define the staff responsible for inputting the manual records.

Recommendation 3: Create an offline file of resident records—including medication administration, physician orders, and treatment records—that can be accessed if the EMR or organization's cyber systems are unavailable.

NIST Function: Protect (information protection processes and procedures)

Observation: Many participants identified the need to develop and/or improve employees' cybersecurity training to better protect facility data and information.

Analysis: Many facilities have not conducted adequate training for all employees on cybersecurity issues, in part, due to the recent focus on COVID-19 training and regulations. Staff shortages and turnover have also contributed to not having robust cybersecurity training in many facilities. Finally, while some facilities do review cybersecurity in new hire training, particularly with e-mail and password protection, ongoing training is often lacking.

Recommendation 1: Codify cybersecurity training standards and requirements in policy documents, including third-party contracts and service level agreements.

Recommendation 2: Implement onboarding/initial cyber training for all employees within a short timeframe of an employee's start date.

Recommendation 3: Once implemented, maintain a program of cyber training on a regular or annual basis.

NIST Function: Detect (anomalies and events; detection processes)

Observation: Many participants identified the need to develop and/or improve employees' cybersecurity training, especially around how to **detect** potential issues early.

Analysis: While most facilities reported providing a minimal level of cybersecurity training, many facilities do not have a robust program in place. Facilities acknowledge that this creates vulnerabilities that could potentially lead to a cyber incident.

Recommendation 1: Explore the Federal Virtual Training Environment (FedVTE) for additional no-cost, cyber training programs.

Recommendation 2: Review and update policies to ensure that notifications of potential threats to systems are provided in a timely way to system users.

NIST Function: Respond (response planning; analysis; improvements; communications)

Observation: Many participants were uncertain on how to begin or enhance their cyber incident preparation, including where to find planning and cyber threat resources.

Analysis: Although most facilities reported that they had taken a few preliminary steps towards improving their cyber incident preparation, most indicated that identifying additional resources would be valuable to them. They were interested in both written materials such as templates as well as experts who could assist in plan development.

Recommendation 1: Explore resources outlined in Appendix F.

Recommendation 2: Develop a centralized location for plans, policies, procedures, and lists for employees to reference.

Recommendation 3: Maintain hard copies of plans, policies, procedures, and lists to use if the electronic version is inaccessible.

Recommendation 4: Conduct regular cybersecurity exercises and discussions within your organization to further enhance leadership's understanding of the impacts of such incidents.

HPP Capability 2: Health Care and Medical Response Coordination

- *Develop and Coordinate Health Care Organization and Health Care Coalition Response Plans*
- *Coordinate Response Strategy, Resources, and Communications*
- *Utilize Information Sharing Procedures and Platforms*

NIST Function: Identify (risk assessment)

Observation: While some participants, especially those who work within a large corporate structure, believe they have a strong information technology (IT) department, they sometimes consider cybersecurity to be only an IT issue.

Analysis: Some facilities reported that they relied on their IT department to detect and manage any cyber issues that may arise but had not considered impacts related to their ability to care for residents. Reliance on IT was particularly prominent at facilities with large corporate structures but also was an issue raised by smaller facilities that use an outside IT vendor.

Recommendation 1: Work more closely with IT to identify specific risks and vulnerabilities including establishing a regular schedule for IT and the emergency preparedness team to meet to discuss cybersecurity issues.

Recommendation 2: Develop or update policies, procedures, and training to encourage system users to report unusual issues as soon as they are discovered.

NIST Function: Protect (information protection processes and procedures)

Observation: A number of participants indicated that their facility firewall protection was strong and that their IT department or vendor kept up to date on installing security patches.

Analysis: While it's commendable that facilities believe their IT vendor or department is doing everything possible to protect against cyberattacks, it did not appear from the discussions that the emergency preparedness teams were in close contact with the IT team. Working more closely with IT to help them understand the consequences of a cyberattack on the facility's ability to keep residents safe and likewise having IT explain the vulnerabilities they are tracking can help better prepare for potential impacts.

Recommendation: Coordinate with IT vendor or department to ensure they are maintaining firewalls and system patches as a defense against cyberattacks, including creating and maintaining an update verification schedule.

NIST Function: Detect (anomalies and events; detection processes)

Observation: Many participants indicated the need to improve staff and leadership knowledge about potential vulnerabilities, e.g., password protection, email phishing schemes.

Analysis: Many facilities acknowledged that they had not been providing enough training and information to staff about cybersecurity, especially given the focus on COVID-19 over the past several

years. A number of facilities also mentioned the need to involve leadership in cybersecurity awareness and training so they can make informed decisions if there is an incident, as well as to develop response policies in advance.

Recommendation: Provide routine training and testing of all staff, including leadership, on cybersecurity.

NIST Function: Respond (analysis; improvements; communications; response planning)

Observation: Some participants were uncertain of the cyber incident reporting requirements in their vendor contracts.

Analysis: Many facilities were unsure generally of their requirements to report cyber incidents. Many were not familiar with the contents of their vendor contracts, including reporting requirements. Additionally, many facilities were not certain about regulatory requirements to report incidents or whether they should report cyber incidents to law enforcement. There was also uncertainty about to whom the report be made.

Recommendation 1: Review vendor contracts to identify reporting and notification requirements for cyber incidents, including thresholds and timelines.

Recommendation 2: Ensure these requirements are outlined within the organization's incident response plan.

Recommendation 3: Ensure future contracts contain standardized cybersecurity reporting requirements.

HPP Capability 3: Continuity of Health Care Service Delivery

- *Identify Essential Functions for Health Care Delivery*
- *Plan for Continuity of Operations*
- *Develop Strategies to Protect Health Care Information Systems and Networks*
- *Coordinate Health Care Delivery System Recovery*

NIST Function: Identify (risk assessment; risk management strategy)

Observation: Many participants had not considered a cascading impact of a cyberattack that could affect facility systems beyond EMRs.

Analysis: One of the scenarios presented a situation where the cyber incident initially observed in EMR systems also affected other systems within the facility. Participants tended to be focused primarily on managing the situation with the EMR system without considering the risk to resident safety if other systems were also impacted. Participants did identify impacts to clinical services as being important but many did not address concerns related to compromises to the building's systems.

Recommendation 1: Work with IT to examine all networked devices and identify potential vulnerabilities.

Recommendation 2: Ensure that other essential functions such as meal preparation and pharmacy needs are considered in cybersecurity policies and plans, including procedures and training on early detection of potential issues for these functions.

NIST Function: Protect (information protection and procedures)

Observation: Many participants indicated that their current cybersecurity policies, procedures, and plans require a review and update to address potential incidents.

Analysis: Most facilities have a cybersecurity policy and plan, but many felt that they were not as robust or up to date as they could be. One of the clearest lessons learned expressed during the discussions was on the importance of reviewing and ensuring the plans, policies, and procedures are comprehensive, and that staff at all levels, including leadership, are familiar with the contents.

Recommendation 1: Develop a plan to review and revise current cybersecurity emergency plans.

Recommendation 2: Ensure that any changes to cybersecurity plans are shared with leadership and staff and that adequate training on new policies and procedures is provided.

NIST Function: Detect (anomalies and events; detection processes)

Observation: Participants were not always focused on identifying issues affecting systems other than the EMRs, especially those impacting building systems, such as the HVAC system, or a cyberattack that originates with vendors of networked systems and which then propagates into the facility's systems.

Analysis: Participants understood that threats to EMR systems were critically important to the health and well-being of their residents. They were less mindful of the importance of other systems that also have a vital impact on the ability of facilities to keep their residents safe and well.

Recommendation 1: Provide training for staff that helps them detect when systems might be compromised due to a cyberattack versus a mechanical issue, and how to protect devices and systems not yet affected.

Recommendation 2: Ensure that system vendors and devices that use facility networks are not introducing cybersecurity issues into the facility.

NIST Function: Respond (analysis; improvements; communications; response planning)

Observation: Some organizations' incident response plans lack cyber-related communications policies or current contact information for key internal personnel and external organizations.

Analysis: Many facilities indicated that they did not maintain a list of contacts that they should communicate with during a cyber incident. Additionally, facilities reported that they had not prepared a comprehensive set of messages that could be sent to internal and external stakeholders. Some facilities mentioned that some messages exist within departments in the facility but that they lacked a coordinated approach to develope messaging content, how to share information, or maintaining a consistent and up-to-date contact list.

Recommendation 1: Develop pre-approved messages for employees, residents, and media during a potential cyber incident with few specific details that allow your organization time to investigate the incident. Use Ready.gov as a reference for these messages.

Recommendation 2: Maintain up-to-date contact information with primary and alternate points of contact for internal and external notifications.

Recommendation 3: Establish and socialize an employee communications policy governing employees' response to media inquiries or posting information about the organization on social media. Include key elements of the policy in internal incident communications.

NIST Function: Recover (recovery planning; improvements; communications)

Observation: Many participants were unsure about resources that could assist in recovery or indicated they might be hesitant to contact those resources.

Analysis: Facilities indicated that even when they knew they could and should contact law enforcement and other agencies about cyber incidents, they did not have specific contact information for people at these organizations. A best practice of emergency preparedness is to establish relationships with organizations that facilities will need to interact with before any incident occurs.

Recommendation: Facilities should establish relationships with organizations that could assist in recovery planning before an incident occurs.

APPENDIX A: IMPROVEMENT PLAN

The Improvement Plan is intended to help facilities which participated in the New York City Long-Term Care Cybersecurity Tabletop Exercise track the implementation of recommendations and corrective actions for each area of improvement identified in the exercise. Facility stakeholders should collaborate to identify corrective actions, responsible departments, points of contact, and target start and completion dates for each item.

HPP Capability 1: Foundation for Health Care and Medical Readiness

NIST Function: Identify (risk assessment)

Observation: If an EMR provider is offline for an extended period, facilities are unable to access resident records.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider assessing and defining EMR downtime procedures and capabilities to safely conduct resident care and confirm resident information if the EMR is offline.					
Consider evaluating the time required for staff to input manual resident records into the EMR when the system is restored and allocating and incorporating that amount of time in incident response and recovery planning. Ensure the planning materials define the staff responsible for inputting the manual records.					
Consider creating and maintaining an offline file of resident records, including medication administration, physician orders, and treatment records, that can be accessed if the EMR or organization's cyber systems are unavailable.					

NIST Function: Protect (information protection processes and procedures)

Observation: Many participants identified the need to develop and/or improve employees' cybersecurity training.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider codifying cybersecurity training standards and requirements in facility policy documents, including third-party contracts and service level agreements.					
Consider implementing onboarding and/or initial cyber training for all employees within a short timeframe of an employee's start date.					
Consider establishing and maintaining a program of cyber training on a regular or annual basis once initial cyber training for all new employees has been implemented.					

NIST Function: Detect (anamolies and events; detection processes)

Observation: Many participants identified the need to develop and/or improve employees' cybersecurity training.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider exploring and utilizing the Federal Virtual Training Environment (FedVTE) and other Federal, State, and local resources for no- or low-cost cyber training programs.					

NIST Function: Respond (response planning; analysis; improvements; communications)

Observation: Many participants were uncertain on how to begin or enhance their cyber incident preparation, including where to find planning and cyber threat resources.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider reviewing and updating policies as needed to ensure that notification of potential threats to systems are provided in a timely way to system users.					
Consider exploring and utilizing the resources outlined in Appendix F for further information on developing and enhancing a cyber incident preparedness program.					
Consider developing a centralized location for plans, policies, procedures, and lists with access for all employees to reference.					
Consider maintaining hard copies of plans, policies, procedures, and lists to use if the electronic versions are inaccessible.					

HPP Capability 2: Health Care and Medical Response Coordination

NIST Function: Identify (risk assessment)

Observation: While some participants, especially those who work within a large corporate structure, believe they have a strong IT department, they sometimes consider cybersecurity to be only an IT issue.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider having the facility emergency preparedness team work more closely with IT to identify specific risks and vulnerabilities, including establishing a regular schedule for IT and the emergency preparedness team to meet to discuss cybersecurity issues.					
Consider developing or updating policies, procedures, and training to encourage system users to report unusual issues as soon as they are discovered.					

NIST Function: Protect (information protection processes and procedures)

Observation: A number of participants indicated that their facility firewall protection was strong and that their IT department or vendor kept up-to-date on installing security patches.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider coordinating with the facility's IT vendor or department to ensure they are maintaining firewalls and system patches as a defense against cyberattacks, including creating and maintaining an update verification schedule.					

NIST Function: Detect (anomalies and events; detection processes)

Observation: Many participants indicated the need to improve staff and leadership knowledge about potential vulnerabilities, e.g., password protection, e-mail phishing schemes.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider developing and providing a routine training program and regular testing of all staff, including leadership, on cybersecurity.					

NIST Function: Respond (analysis; improvements; communications; response planning)

Observation: Some participants were uncertain of the cyber incident reporting requirements in their vendor contracts.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider reviewing vendor contracts to identify reporting and notification requirements for cyber incidents, including thresholds and timelines.					
Consider ensuring these requirements are outlined within the organization's incident response plan.					
Consider ensuring future contracts with IT vendors and other vendors contain standardized cybersecurity reporting requirements.					

HPP Capability 3: Continuity of Health Care Service Delivery

NIST Function: Identify (risk assessment; risk management strategy)

Observation: Many participants had not considered a cascading impact of a cyberattack that could affect facility systems beyond EMRs.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider working with your facility IT department or vendor to examine all networked devices and identify potential vulnerabilities.					
Consider ensuring that other essential functions such as meal preparation and pharmacy needs are identified and addressed in cybersecurity policies and plans, including procedures and training on early detection of potential issues for these functions.					

NIST Function: Protect (information protection and procedures)

Observation: Many participants indicated that their current cybersecurity policies, procedures, and plans require a review and update to address potential incidents.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider developing a plan to review and revise current cyber-security emergency plans on a regular basis.					
Consider ensuring that any chang-es to any cybersecurity plans are shared with leadership and staff and that adequate training on new policies and procedures is provided.					

NIST Function: Detect (anomalies and events; detection processes)

Observation: Participants were not always focused on identifying issues affecting systems other than the EMRs, especially those impacting the building systems such as the HVAC system or a cyberattack that affects system vendors thereby impacting the facility's systems.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider providing training for staff that helps them detect when systems might be compromised due to a cyberattack versus a mechanical issue and how to protect devices and systems not yet affected.					
Consider whether system vendors and devices that use facility networks are secure so that they don't introduce cybersecurity issues into the facility.					

NIST Function: Respond (analysis; improvements; communications; response planning)

Observation: Some organizations' incident response plans lack cyber-related communications policies or current contact information for key internal personnel and external organizations.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider developing pre-approved messages for employees, residents, patients, and media during a potential cyber incident, with few specific details to allow your organization time to investigate the incident. Ready.gov can be used as a reference for these messages.					

Observation: Some organizations' incident response plans lack cyber-related communications policies or current contact information for key internal personnel and external organizations.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider maintaining up-to-date contact information with primary and alternate points of contact for internal and external notifications.					
Consider establishing and socializing an employee communications policy governing employees' response to media inquiries or posting information about the organization on social media and include key elements of the policy in internal incident communications.					

NIST Function: Recover (recovery planning; improvements; communications)

Observation: Many participants were unsure about resources that could assist in recovery or indicated they might be hesitant to contact those resources.					
Recommendation	Corrective Action	Responsible Department	Point of Contact	Start Date	Completion Date
Consider establishing relationships with organizations that could assist in recovery planning before an incident occurs.					

APPENDIX B: FEEDBACK FORM ANALYSIS

At the end of the New York City Long-Term Care Cybersecurity TTX, participants were given the opportunity to provide exercise feedback using an online participant feedback form accessible using a link or QR code. In total, 84 forms were collected and analyzed by exercise staff to gain exercise and conference design feedback, identify key strengths and areas for improvement, and determine future training and exercise recommendations.

Exercise Design

Participants were provided with the following rating chart to evaluate the exercise according to specific assessment factors. Note that not all participants completed an evaluation. The responses were aggregated from the 84 participant feedback forms received and then averaged. This average is provided in the Weighted Average column.

Table 1: Exercise Feedback from Participant Evaluations

Assessment Factor	Strongly Disagree				Strongly Agree	Weighted Average
Feedback	1	2	3	4	5	
Standard Exercise Feedback						
How would you rate this exercise overall?	0	0	4	26	56	4.60
The exercise facilitators were well prepared and knowledgeable	1	0	3	22	60	4.63
The exercise materials (presentations, handouts, surveys/polls, etc.) added value to the exercise.	2	0	9	29	39	4.30
Based on my experience, I would recommend similar exercises to colleagues or other relevant professionals.	1	2	2	28	47	4.48
Based on my participation in this exercise, I will be better prepared to execute my role in preventing, protecting against, responding to, and/or mitigating threats or incidents.	1	1	3	36	38	4.38
Based upon its participation in this exercise, my organization will take steps to enhance its preparedness to execute its role in preventing, protecting against, responding to, and/or mitigating threats or incidents.	1	0	7	27	40	4.40

Assessment Factor	Strongly Disagree				Strongly Agree	Weighted Average
Feedback	1	2	3	4	5	
Feedback on Exercise Objectives						
Objective 1. Examine the plans and abilities of New York City long-term care facilities to respond to a significant cyber incident.	0	0	2	32	51	4.58
Objective 2. Evaluate the ability of New York City long-term care facilities to gather and disseminate essential elements of information during a significant cyber incident.	1	1	5	33	38	4.36
Objective 3. Explore processes to request incident response resources.	1	1	4	33	40	4.39
Objective 4. Explore New York City long-term care facilities' processes for internal and external messaging during a cyber incident.	1	1	1	33	43	4.47
Objective 5. Discuss members' plans, processes, and procedures to recover from a significant cyber incident.	1	1	3	29	45	4.47

Table 2: Participant Exercise Roles

Role	Individual Long-Term Care Representatives	Observers, Planners, Evaluators, Staff	Long-Term Care Facilities
Number of Participants	218	48	72 (68 nursing homes, 4 adult care facilities)

APPENDIX C: PARTICIPANT COMMENTS

Participants completing the exercise evaluation were asked to provide comments on strengths and areas for improvement observed during the exercise and general comments pertaining to the exercise as a whole. Combined participant feedback on each question is presented below.

Table 3: Long-Term Care Facilities' Self-Assessment of Strengths

Topic	Comments
Emergency Plans	Many participants cited their emergency plans as a strength of their organization in guiding their response to and recovery from cybersecurity incidents. A number of participants also specified aspects of their emergency plans as a strength including: • Backup and recovery plans for IT systems and for operational alternatives should systems become compromised • Response plans to provide prioritization of activities • Communications plans internally and with external organizations • Continuity plans, especially continuity of resident care
Vulnerability Awareness	Many facilities indicated that having an awareness of their vulnerability to cyberattacks is a strength that allows them to focus attention on where to improve their systems and training.
IT Systems and Department	Facilities indicated many strengths related to their IT systems and departments including: • A strong IT team in place • Strong firewall protection, along with security updates, to prevent attacks from occurring • Built-in redundancy of IT systems • Limiting networked devices was seen as a way to prevent an attack in one part of the system from cascading into other systems and devices
Teamwork	Participants emphasized the value of team members working together to address cybersecurity concerns. Specific considerations were expressed, including: • Internal communications • Support provided to individual facilities through the larger corporate structure • Discussions and knowledge sharing, including knowledge gained through exercises
Resources	Exercise attendees cited the availability of resources (documentation and plans) and partner organizations to call should they experience an attack, as a strength.

Table 4: Long-Term Care Facilities' Self-Assessment of Areas of Improvement

Topic	Comments
Training	Participants cited training as the most significant area of improvement for their facilities. Specifically, they focused on: • Recognizing and reporting potential cybersecurity issues • Promoting safe computer use • Reviewing downtime procedures including manual systems • Ensuring cybersecurity training is a core competency and is not delayed due to other issues, such as COVID-19
Response Plan Review	Participants recognized the value of reviewing and updating response plans for cybersecurity to ensure continuity of business operations.

Topic	Comments
Review of Downtime Procedures	Participants noted that reviewing and revising downtime procedures is crucial, including training on manual processes. They noted the following areas as needing attention: • Meal ticketing • Payroll • Pharmacy • Adequate supplies
Mass Notification System	Attendees discussed the need for mass notification systems that were not reliant on their e-mail and other networks. They noted the need to secure a mass notification system to use mass texts as a potential option.
Cybersecurity Policy Review	Participants addressed the need to review and implement cybersecurity policies in advance of any potential incident. Facilities with current policies noted their policies required updating.
Vendor Relationships	Participants noted numerous opportunities to improve relationships with vendors and review the resources they might offer. These opportunities include: • Jointly reviewing IT vendor cybersecurity plans for their facility • Examining their facility policy for reliance on IT vendors • Ensuring that contact information for vendors is kept up to date • Reviewing their cybersecurity insurance policies • Strengthening partnerships with IT vendors and other cybersecurity resources
Communication Scripts	Facilities noted the value of pre-scripted messaging to be used in the event of a cyber incident.
IT System Review	Participants described the need to review their IT systems, including inventorying their backup servers, understanding their networked devices and defining the reach of impact to networks, and examining reporting thresholds.
Backup Systems	Attendees addressed ways to review backup systems, including: • Examining the backup process for all systems at all levels, including meal ticketing and pharmacy • Reviewing the frequency of backups • Retention policy for backups
Communication Plans	Participants indicated that both internal and external communication plans require review and updates to take potential cybersecurity incidents into account.
Leadership Knowledge	Attendees discussed the need for improved knowledge among leadership about the potential for and the impact of cybersecurity incidents on their business and the ability to maintain resident care levels.
Cybersecurity Resources	Participants expressed a desire for additional outside resources on cybersecurity, including documentation and contact information for expertise.
Drills	Participants recognized the value of conducting drills to identify gaps in their knowledge, policies, and procedures, and to improve staff awareness of cybersecurity issues.

APPENDIX D: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY FUNCTIONS/HOSPITAL PREPAREDNESS PROGRAM CAPABILITY CROSSWALK[1]

Exercise Objective	NIST Functions	HPP Capability and Objectives

Objective 1: Examine the plans and abilities of New York City long-term care facilities to respond to a significant cyber incident.	• Identify
	• Protect
	  ◦ PR-IP Information Protection Processes and Procedures
	• Respond
	  ◦ RS.RP Response Planning
	  ◦ RS.AN Analysis
	  ◦ RS.IM Improvements
		• Capability 1: Foundation for Health Care and Medical Readiness
		  ◦ Objective 2: Identify Risks and Needs
		  ◦ Objective 4: Train and Prepare the Health Care and Medical Workforce
		  ◦ Objective 5: Ensure Preparedness is Sustainable
		• Capability 2: Health Care and Medical Response Coordination
		  ◦ Objective 1: Develop and Coordinate Health Care Organization and Health Care Coalition Response Plans
		  ◦ Objective 3: Coordinate Response Strategy, Resources, and Communications
		• Capability 3: Continuity of Health Care Service Delivery
		  ◦ Objective 1: Identify Essential Functions for Health Care Delivery

Objective 2: Evaluate the ability for New York City long-term care facilities to gather and disseminate essential elements of information during a significant cyber incident.	• Identify
	  ◦ ID.RA Risk Assessment
	• Detect
	  ◦ DE.AE Anomalies and Events
	  ◦ DE.DP Detection Processes
	• Respond
	  ◦ RS.CO Communications
		• Capability 1: Foundation for Health Care and Medical Readiness
		  ◦ Objective 2: Identify Risks and Needs
		  ◦ Objective 4: Train and Prepare the Health Care and Medical Workforce
		  ◦ Objective 5: Ensure Preparedness is Sustainable
		• Capability 2: Health Care and Medical Response Coordination
		  ◦ Objective 1: Develop and Coordinate Health Care Organization and Health Care Coalition Response Plans
		  ◦ Objective 2: Utilize Information Sharing Procedures and Platforms
		  ◦ Objective 3: Coordinate Response Strategy, Resources, and Communications
		• Capability 3: Continuity of Health Care Service Delivery
		  ◦ Objective 1: Identify Essential Functions for Health Care Delivery

1 The National Institute of Standards and Technology (NIST) Cybersecurity Framework (https://www.nist.gov/cyberframework); The Hospital Preparedness Program (HPP) (https://www.phe.gov/preparedness/planning/hpp/reports/documents/2017-2022-healthcare-pr-capablities.pdf).

Exercise Objective	NIST Functions	HPP Capability and Objectives

Objective 3: Explore processes to request incident response resources.	• Respond
	  • RS.RP Response Planning
	  • RS.CO Communications
	  • RS.IM Improvements
		• Capability 1: Foundation for Health Care and Medical Readiness
		  • Objective 2: Identify Risks and Needs
		  • Objective 5: Ensure Preparedness is Sustainable
		• Capability 2: Health Care and Medical Response Coordination
		  • Objective 1: Develop and Coordinate Health Care Organization and Health Care Coalition Response Plans
		  • Objective 2: Utilize Information Sharing Procedures and Platforms
		  • Objective 3: Coordinate Response Strategy, Resources, and Communications
		• Capability 3: Continuity of Health Care Service Delivery
		  • Objective 1: Identify Essential Functions for Health Care Delivery

Objective 4: Explore New York City long-term care facilities' processes for internal and external messaging during a cyber incident.	• Identify
	  • ID.RA Risk Assessment
	• Respond
	  • RS.RP Response Planning
	  • RS.CO Communications
	  • RS.IM Improvements
		• Capability 1: Foundation for Health Care and Medical Readiness
		  • Objective 2: Identify Risks and Needs
		  • Objective 5: Ensure Preparedness is Sustainable
		• Capability 2: Health Care and Medical Response Coordination
		  • Objective 1: Develop and Coordinate Health Care Organization and Health Care Coalition Response Plans
		  • Objective 2: Utilize Information Sharing Procedures and Platforms
		  • Objective 3: Coordinate Response Strategy, Resources and Communications
		• Capability 3: Continuity of Health Care Service Delivery
		  • Objective 1: Identify Essential Functions for Health Care Delivery

Objective 5: Discuss members' plans, processes, and procedures to recover from a significant cyber incident.	• Identify
	  • ID.RA Risk Assessment
	  • ID.RM Risk Management Strategy
	• Recover
	  • RC.RP Recovery Planning
	  • RC.IM Improvements
	  • RC.CO Communications
		• Capability 3: Continuity of Health Care Service Delivery
		  • Objective 1: Identify Essential Functions for Health Care Delivery
		  • Objective 2: Plan for Continuity of Operations
		  • Objective 4: Develop Strategies to Protect Health Care Information Systems and Networks
		  • Objective 7: Coordinate Health Care Delivery System Recovery

APPENDIX E: PARTICIPATING ORGANIZATIONS

- Federal
  - Federal Bureau of Investigation
  - US Cybersecurity and Infrastructure Security Agency
- State
  - New York State Department of Health
- Local
  - New York City Cyber Command
  - New York City Department of Health and Mental Hygiene
  - New York City Emergency Management
  - New York City Police Department
- Non-Governmental Organizations
  - Centers Health Care
  - Healthix
  - Incident Management Solutions, Inc.
  - Greater New York Health Care Facilities Association
  - Greater New York Hospital Association
  - Southern New York Association
- New York City Nursing Homes and Adult Care Facilities
  - April 26, 2022 – Morning Session
    - Atrium Center for Rehabilitation and Nursing
    - Bensonhurst Center for Rehabilitation and Healthcare
    - Bronx Park Rehabilitation & Nursing Center
    - Brooklyn United Methodist Church Home
    - Carmel Richmond Healthcare and Rehabilitation Center
    - Casa Promesa
    - Cliffside Rehabilitation & Residential Health Care Center
    - Downtown Brooklyn Nursing & Rehabilitation Center
    - Elmhurst Care Center
    - Forest Hills Care Center
    - Haven Manor Health Care Center
    - Jeanne Jugan Residence
    - Margaret Tietz Nursing and Rehabilitation Center
    - Methodist Home for Nursing and Rehabilitation
    - Norwegian Christian Home and Health Center
    - NYC Health + Hospitals/Carter
    - NYC Health + Hospitals/Gouverneur
    - NYC Health + Hospitals/McKinney
    - NYC Health + Hospitals/SeaView

- Ozanam Hall of Queens Nursing Home
- Queen of Peace Residence
- Queens Nassau Rehabilitation and Nursing Center
- Rebekah Rehab and Extended Care Center
- Rockaway Care Center
- Sheepshead Nursing & Rehabilitation Center
- Shore View Nursing and Rehabilitation Center
- St. Mary's Center
- St. Mary's Hospital for Children
- Upper East Side Rehabilitation and Nursing Center
- VillageCare Rehabilitation and Nursing Center

- April 26, 2022 – Afternoon Session
  - Amsterdam Nursing Home
  - Bainbridge Nursing & Rehabilitation Center
  - Buena Vida Rehabilitation and Nursing Center
  - Caring Family Nursing and Rehabilitation Center
  - Crown Heights Center for Nursing and Rehabilitation
  - Eger Health Care and Rehabilitation Center
  - Fort Tryon Center for Rehabilitation and Nursing
  - Golden Gate Rehabilitation & Health Care Center
  - Grand Manor Nursing & Rehabilitation Center
  - Hillside Manor Rehabilitation and Extended Care Center
  - Jamaica Hospital Nursing Home
  - Lawrence Nursing Care Center
  - Linden Center for Nursing and Rehabilitation
  - Manhattanville Health Care Center
  - Meadow Park Rehabilitation and Health Care Center
  - New Carlton Rehab and Nursing Center
  - New Glen Oaks Nursing Home
  - New Vanderbilt Rehabilitation and Care Center
  - New York Congregational Nursing Center
  - Oceanview Nursing & Rehabilitation Center
  - Park Inn Home
  - Pelham Parkway Nursing Home and Rehabilitation Facility
  - Providence Rest
  - Rutland Nursing Home
  - Sapphire Center for Rehabilitation and Nursing of Central Queens
  - Spring Creek Rehabilitation & Nursing Care Center
  - St Patrick's Home
  - Saints Joachim & Anne Nursing and Rehabilitation Center

    - The New Jewish Home University Avenue Assisted Living
    - The Pavilion at Queens for Rehabilitation and Nursing
    - The Wayne Center for Nursing & Rehabilitation
    - University Avenue Assisted Living
    - Wavecrest Home for Adults
- April 27, 2022 – Morning Session
    - Beach Gardens Rehab and Nursing Center
    - BronxCare Special Care Center
    - Hopkins Center for Rehabilitation and Healthcare
    - Isabella Geriatric Center
    - Laconia Nursing Home
    - Moffat Gardens ALP
    - NYC Health + Hospitals / Coler
    - Rego Park Nursing Home
    - The New Jewish Home

APPENDIX F: RECOMMENDED RESOURCES

The following resources—available from the US Federal government, New York State, and New York City—provide detailed information and data on cybersecurity.

Resource	Website
Federal Resources	
Resources to develop or improve the organization's cyber incident response plan • The Cybersecurity and Infrastructure Security Agency (CISA)'s Cyber Resilience Review Resource Guide • NIST resources	Cyber Resilience Review Resource Guide: https://www.cisa.gov/uscert/resources/assessments NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
Contact CISA Region 2 personnel to explore: • CISA's no-cost cyber hygiene resources and services • CISA's free cybersecurity tools	https://www.cisa.gov/region-2 Regional Office: cisaregion2@hq.dhs.gov After hours: • For more questions on this topic or CISA in general, please contact central@cisa.gov • To report anomalous cyber activity and/or cyber incidents 24/7 email report@cisa.gov or (888) 282-0870
CISA publication: *Preparing for and Mitigating Potential Cyber Threats*, December 15, 2021 • Includes links to resources	https://www.cisa.gov/sites/default/files/publications/CISA_INSIGHTS-Preparing_For_and_Mitigating_Potential_Cyber_Threats-508C.pdf
2021 Top Routinely Exploited Vulnerabilities from CISA	https://www.cisa.gov/uscert/ncas/alerts/aa22-117a
Sign up for CISA Alerts *(Alerts provide timely information about current security issues, vulnerabilities, and exploits.)*	For information: https://www.cisa.gov/uscert/ncas/alerts To sign up: https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new
New York State Resources	
New York State Police	https://troopers.ny.gov/
New York State Intelligence Center (NYSIC) *(The New York State Intelligence Center is a multi-agency, all-crimes fusion center, that identifies, prevents, and protects New York against emerging domestic and international terrorist and criminal threats through information collection, analysis, and dissemination of intelligence. The NYSIC provides investigative and analytic resources, subject matter expertise, and information in an effort to detect, prevent and respond to both criminal and terrorist activity.)*	https://troopers.ny.gov/counter-terrorism

Resource	Website
New York City Resources	
New York City Cyber Command (NYC3)	https://www1.nyc.gov/site/cyber/about/about-nyc-cyber-command.page Information on downloading the NYC3 Secure App: https://www1.nyc.gov/site/cyber/index.page#:~:text=The%20NYC%20Secure%20app%20is,how%20to%20address%20the%20threats
Other Resources	
Multi-State Information Sharing and Analysis Center (MS-ISAC) *(The mission of the MS-ISAC is to improve the overall cybersecurity posture of US State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication.)*	https://www.cisecurity.org/ms-isac
Health Information Sharing and Analysis Center's (H-ISAC) *(Health-ISAC is a trusted community of critical infrastructure owners and operators within the Healthcare and Public Health sector (HPH). The community is primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities that can include data such as indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors, advice and best practices, mitigation strategies and other valuable material.)*	https://h-isac.org/
Healthcare Sector and Public Health Sector Coordinating Council (HSCC): Operational Continuity – Cyber Incident	https://healthsectorcouncil.org/occi/
HHS 405(d) Data Security guides for different sized organizations	HHS 405(d) organization: https://405d.hhs.gov/ • How to: Implement Data Security – Small • How to: Implement Data Security – Medium • How to: Implement Data Security – Large
Healthix: Policies, Privacy, Security	https://healthix.org/who-we-are/privacy-and-security-2/

APPENDIX G: ACRONYMS

Acronym	Definition
AAR	After-Action Report
CIRP	Cyber Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
DHS	US Department of Homeland Security
DOHMH	New York City Department of Health and Mental Hygiene
DOH	New York State Department of Health
EHR	Electronic Health Record
EMR	Electronic Medical Record
FBI	Federal Bureau of Investigation
FedVTE	Federal Virtual Training Environment
FEMA	Federal Emergency Management Agency
GNYHCFA	Greater New York Health Care Facilities Association
GNYHA	Greater New York Hospital Association
HICP	Health Industry Cybersecurity Practices
HPP	Hospital Preparedness Program
IP	Improvement Plan
IT	Information Technology
NCEPP	National Cyber Exercise and Planning Program
NIST	National Institute of Standards and Technology
PHI	Protected Health Information
PII	Personally Identifiable Information
SLTT	State, Local, Territorial, and Tribal
SME	Subject Matter Expert
SNYA	Southern New York Association
TLP	Traffic Light Protocol
TTX	Tabletop Exercise