Cyber-Attack Emergency Response Plan

New York City Department of Health

Long Island City, New York, USA

James Abruzzo, Haoan Chen and Nancy Hu

GPH-GU 5150 Emergency Preparedness for Healthcare Organizations
June 25, 2024

Table of Contents

III. Preface …………………………………………………………………………………….. 3

IV. Signature Page ...………………………………………………………………………..... 4

V. Mission Statement …………………………………………………………………………...... 5

Statement of Purpose ...……………………………………………………………….. 5

Authorities ...…………………………………………………………………………….. 6

Definitions …………………………………………………...………………………….. 7

Communication Plans ………………………………………...…………………….…..... 8

Mutual Aid Agreement ………………………………………………………………… 9

IV: Public Health Concept of Operations ...…………………………………………………... 10

References ………………………………………………………………………………...... 14

Annex 1: Threat and Hazards Assessment Table (THIRA) ……………………………………. 17

Annex 2: Training Plan ……………………………………………………………………….. 18

Part III: Preface

The charge of the New York City Department of Health and Mental Hygiene (NYC DOH) is to ensure the health and well-being of over 8 million residents amidst one of the most populous and diverse cities in the world. This plan is specifically focused on the NYC DOH and outlines the steps to be taken in the event of a cyber-attack targeting the department. New York City has the most extensive public healthcare system in the United States, providing services to a wide and varied population, including many from the most vulnerable and underserved communities.

Cybersecurity threats have dramatically increased over the past couple of years, including threats to critical CISA infrastructure such as healthcare.[1] Cyber-attacks on hospitals and healthcare systems have significant impacts on patient care, hospital finances and hospital infrastructure.[2] This plan focuses specifically on the steps to be taken if a cyber-attack targets the NYC DOH. The primary emphasis will be on the communication strategies during the event to ensure effective and timely dissemination of information. Cyber-attacks against NYC Health and Hospitals would pose a significant risk to sensitive patient data, the integrity of healthcare operations, and consequently, public trust towards that system. Its effects could lead to a vital healthcare delivery interruption, patient care breach, and loss of lives. For example, a cyberattack on over 43,000 patients from the NYC Health and Hospitals System exposed PHI in ways such as names, dates of birth, and prescription information.[4] Although there was no evidence of data misuse, the breach highlighted the vulnerabilities in the system. Likewise, a ransomware attack on the Brooklyn Hospital Center resulted in, among other things, the permanent deletion of patient information, including names and some medical imaging, causing significant operational disarray; the hospital had to return to manual hardcopy record-keeping and redirect emergency functions.[4]

Due to its large population, and outsized role not only as the largest and most influential American metropolis, but also for its role as the global center of finance and commerce, culture and technology, entertainment and media, academics and scientific output and cutting-edge healthcare, and the arts and fashion, and home to the headquarters of the United Nations. New York City is immeasurably important to the US and to the world. Cyber-attacks on any of its key infrastructure can have rippling effects throughout the economy and population. With its large and highly diverse population, NYC relies on its outstanding public health and public health care systems to help deliver high quality care to over a million New Yorkers each year. Response to disruptions in critical communications that might be caused by cyber-attacks are complicated by the fact that over 800 languages are spoken in NYC.[3] Many public health sector patients in NYC are recent immigrants, non-English speakers, and individuals living in poverty. This presents a challenge in developing an effective channel of communication and ensuring prompt action when communications systems are damaged or held hostage during a cyber-attack. With the critical role the NYC Health and Hospitals System plays in caring for millions of New Yorkers, the development of a robust and all-inclusive response plan on preventing cyber-attacks is essential. The new plan will enhance resiliency and result in the protection of sensitive information with an assurance of continuity in care in the face of cyber threats.

Part IV: Signature Page

My signature below indicates that I have read the New York City Department of Health Cyber Attack Emergency Response Plan and agree to support the adoption and implementation of the plan as it is written.

NYC Department of Health and Mental Hygiene

Ashwin Vasan, MD, PhD, Commissioner Date

Emiko Otsubo, MSW, Chief Operating Officer Date

Julie Friesen, MS, Deputy Commissioner, Administration Date

Scott Liu, Chief Information Officer, Information Technology Date

Beth Maldin, MPH, Deputy Commissioner, Emergency Preparedness & Response Date

NYC Office of Technology & Innovation

Matthew C. Fraser, Chief Technology Officer Date

NYC Office of Emergency Management

Zachary Iscol, Commissioner Date

Part V: Mission Statement

The mission of the New York City Department of Health and Mental Hygiene (NYC DOH) is to protect and promote the health of all New Yorkers.[3] The vision for the NYC DOH is a city where all New Yorkers can realize their full health potential regardless of who they are, how old they are, where they come from or what neighborhood they live in. The values the NYC DOH holds in following its mission and vision are accountability, compassion, equity, excellence, integrity, rigor and transparency.[3]

Statement of Purpose

The purpose of this plan is to ensure that New York City's Department of Health is equipped with the necessary procedures to identify and adequately respond to a cyber-attack on its systems or a health care entity that operates within its jurisdiction. These procedures are designed to minimize the scope of any attack and limit any breach, disruption of services and amount of personal health information (PHI) or other protected information hacked from the system. This plan will provide a plan of action on steps that need to be taken as soon as an attack occurs, who should be contacted, what steps that need to be taken as soon as an attack occurs, who should be contacted and who will be responsible throughout the department for overseeing and communicating these directives to all pertinent stakeholders. Not all cyber-attacks are created equal; some may not penetrate systems or only a small subset of users may be impacted, while larger scale attacks may result in the system unable to deliver critical services as a result. For any cyber-attack on the NYC DOH systems, this plan will delineate the response and recovery activities that should take place.

Authorities

Health Insurance Portability and Accountability Act (HIPAA): An act at the federal level, and it is very significant in assuring protection for patient health information. It provides national standards for electronically protecting ePHI in the healthcare industry. It therefore forms the platform over which the security of data controlled from unauthorized access and breaches is handled.

New York State Cyber Security Policy: New York State has taken significant steps to fortify its cybersecurity defenses. Governor Kathy Hochul has recently unveiled an all-inclusive cybersecurity strategy aimed at securing the digital infrastructure in the state. This includes an investment of $90 million, with $30 million going towards the enhancement of cybersecurity in local governments and $500 million specifically for improving information technology cybersecurity in healthcare. These fund allocations, therefore, underline the undivided efforts of New York in building a resilient cybersecurity framework capable of adapting to the changing threat landscapes.

NYC Office of Technology and Innovation: established via Executive Order 202, is the center of New York City's cyber defense effort. The agency collaborates with many city agencies to prevent, detect, and respond to cyber threats. The NYC Cyber Command leads citywide critical infrastructure protection and sensitive information for the city to stay current and resilient in cybersecurity.

New York State Division of Homeland Security and Emergency Services (DHSES): To coordinate the state's response to cyber threats and incidents, DHSES actively provides available resources, guidance, and expertise in offering critical support for local governments and healthcare systems. Their involvement guarantees that local entities are well-positioned to act in defense against cyber-attacks and can provide proper response efforts if an incident should occur.

Federal Bureau of Investigation (FBI) Cyber Division: The FBI Cyber Division is the most critical partner in all cyber operations. Through seamless coordination with local and state agencies, including NYC Cyber Command and DHSES, the FBI supports major cyber incidents while bringing considerable resources and expertise to bear on cyber-attack investigations and prosecuting cybercriminals.

Definitions

Cyberattack:

A deliberate exploitation of computer systems, technology-dependent enterprises, and networks; uses malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes such as information and identity theft.

PHI (Protected Health Information):

Any information about health status, provision of healthcare, or payment for healthcare that can be linked to an individual. This includes any part of a patient's medical record or payment history.

Phishing:

The attempt to acquire sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication, usually email.

Incident Response Plan (IRP):

A set of instructions and procedures to detect, respond to, and recover from network security incidents. It includes preparation, detection and analysis, containment, eradication, and recovery.

Citywide Incident Management Center (CIMS):

The emergency response system which establishes roles and responsibilities for various departments during an incident response.

Ransomware:

A type of malicious software designed to block access to a computer system until a sum of money is paid. In healthcare, it can lead to loss of access to patient records, thus severely impacting patient care.

Data Breach:

The unauthorized acquisition, access, use, or disclosure of PHI, which compromises the security or privacy of the information. This can result in harm to the individuals whose data was accessed.

Business Continuity Plan (BCP):

A plan for the continuation of operations during and after a disaster. The plan ensures that critical business functions will continue during and after a disaster, including IT disruptions due to cyberattacks.

Disaster Recovery Plan (DRP):

A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. This includes steps to restore data, applications, and IT infrastructure to ensure business continuity.

Communication Plan

In the event of a cyber-attack, the CIMS protocol will be activated to assist with the response effort. The NYC DOH Chief Information Officer will, in consultation with the New York City Department of Innovation and Technology Chief Technology Officer, determine the scope and impact of the attack and declare a cyberattack event has taken place and coordinate the response and communication to the departments and entities impacted.

To ensure rapid and effective communication within the NYC Health and Hospitals System during a cyberattack, multiple methods could be employed to maintain operational integrity and minimize disruption. To put the spotlight on internal communication strategy, firstly, immediate alerts can be sent via text messages and automated calls to staff members' personal and work phones using services like Twilio or SendWordNow.[4,5] Redundancy can be ensured by using multiple channels and confirmation mechanisms. Notifications can also be sent to personal email by using secure services such as ProtonMail or Tutanota with instructions for next steps and updates. ProtonMail employs end-to-end encryption and AES 256-bit encryption to secure emails, along with two-factor authentication (2FA) for added security. It benefits from stringent Swiss privacy laws and provides a user-friendly interface with features such as scheduling emails and auto-destructing messages. Tutanota encrypted emails, attachments, address books, and calendar entries using AES 128-bit and RSA 2048-bit encryption protocols. It supports 2FA and adheres to the General Data Protection Regulation (GDPR) in Germany. It offers a straightforward and highly responsive interface with desktop clients for Windows, macOS, Linux, and mobile apps for Android and iOS. Both services ensure secure and reliable email notifications, which can make them excellent choices for disseminating critical information during a cyberattack.[6,7]

Also, secure internal platforms like Microsoft Teams, Slack, or private intranet portals can be used for continuous updates. These systems will be isolated from compromised networks. Moreover, additional methods include emergency notification apps (e.g., AlertMedia, Everbridge) and digital signage for real-time updates. Backup communication methods such as two-way radios and landline phones will be employed if network systems are down. The IT department can monitor and manage communication systems, while department heads ensure all team members are informed and follow protocols. The Emergency Response Team can coordinate internal communication efforts and ensure all staff are aware of their roles and responsibilities. Communications can include to refrain from accessing particular systems (electronic health records or other impacted or potentially breached databases) and instructions to revert to utilizing paper documentation throughout the duration of the cyber-attack event.

Upon the conclusion of the cyber-attack event, IT systems may reset all user passwords to force users with access to systems to create new passwords when attempting to log back in.

To maintain transparency and coordination with external partners and the public during a cyberattack, the NYC DOH can implement a comprehensive external communication strategy. Specifically, the Public Information Officer (PIO) can manage media relations, which can ensure accurate and timely dissemination of information to maintain public trust and prevent misinformation.[8] Also, regular press releases and media briefings can be issued through official channels including the system's website and social media platforms. Public alerts will be disseminated using the NYC Emergency Alert System for emergency updates. Coordination with partner hospitals, emergency services, and the NYC Department of Health (DOH) can be facilitated through secure communication channels, with regular updates provided to all partners.[9] The IT department can liaise with external cybersecurity experts to ensure all technical information is clearly communicated. Executive leadership can oversee the communication strategy to ensure alignment and information flow across all departments and external partners.

Mutual Aid Agreement

The NYC DOH can establish mutual aid agreements with several key agencies and organizations to ensure a coordinated response, resource sharing, and mutual support in the event of a cyberattack. These include the NYC Office of Emergency Management (OEM) for emergency management and resource allocation, partner hospitals such as New York Presbyterian and Mount Sinai for patient transfer and support, and identity protection services like LifeLock for safeguarding patients' personal information.[10,11] Additional partners include Emergency Medical Services (EMS) for medical response and transportation, local law enforcement agencies for cybersecurity measures and infrastructure protection, and IT and cybersecurity firms for technical support. These agreements guided by FEMA's mutual aid principles and CDC's model agreements can enhance the resilience of the healthcare system by fostering collaboration. They can ensure timely responses and pool resources to strengthen preparedness and response capabilities against cyber threats.[12] The NYC DOH maintains a Memorandum of Understanding with the NYC Office of Technology and Innovation, the agency responsible for protecting all city systems against cyber-attacks and leading the response efforts for any such attacks.

Part VI: Public Health Concept of Operations (CONOPS)

Assessing The Needs of The Population

In the event of a cyber-attack on the NYC Department of Health (NYC DOH), there will be a variety of needs among members of the public who may have been impacted by the attack. It will be imperative for operations of the DOH to quickly determine the extent of the attack, what kinds of records or systems may be at risk, and what protected health information of patients may be exposed. Among the vulnerable populations impacted would be the elderly, disabled, and other at-risk populations who may not be able to access online portals, emails or other electronic forms of communication and instruction, along with those who may not be fluent in English and require translation services. Having call centers capable of handling the response and volume among these patients and with all of the necessary language services typically available will be a critical component of the operational response.

Services provided by the NYC DOH may be disrupted in the event of a cyber-attack and this in turn may hamper operations at a variety of clinics that provide a wide variety of services ranging from community health services and screenings, drug treatment centers and immunizations and tuberculosis evaluations. Other services for vulnerable populations include mental health service outreach and suicide prevention and alcohol and drug abuse service and prevention. All services from clinic care, screenings, education sessions, text-based services, program audits and more will need to ensure that they are each equipped with resources to continue operation without access to electronic systems or databases and able to rely on paper documentation as necessary to carry out their critical services to members of the public including members of vulnerable populations.

United States health systems, including Departments of Health, are supported in their efforts to prevent and respond to cyber-attacks by the U.S. Department of Health and Human Services (HHS) Administration of Strategic Preparedness and Response (ASPR). Since 2015, ASPR has sponsored the Technical Resources, Assistance Center, and Information Exchange (TRACIE). The goal of ASPR TRACIE is to “fill gaps in healthcare system preparedness capabilities by providing timely, innovative ways to share information and promising practices during planning efforts”.[13] ASPIR TRACIE designed this resource to help healthcare facilities, and the systems they may be a part of, to understand the roles and responsibilities of stakeholders before, during and after a cyber incident.

To maintain situational awareness, the NYC DOH will regularly review the following federal sites for up-to-date alerts and guidance:

- Health Sector Cybersecurity Coordination Center (HC3) https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts
- HHS Healthcare and Public Health Sector:
  - https://www.phe.gov/Preparedness/planning/cip/Pages/CIPInquiry.aspx
  - https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts

- HHS 405(d): https://405d.hhs.gov/
- CISA: National Cyber Awareness System Bulletins/Reports; Sign-up for Alerts https://www.cisa.gov/about/contact-us/subscribe-updates-cisa
- CISA: SHIELDS UP webpage https://www.cisa.gov/shields-up
- CISA: Stop Ransomware webpage https://www.cisa.gov/stopransomware

According to the HHS, the following are the top cybersecurity threats and practices for 2023[14]:

Top five cybersecurity threats: 1. Social Engineering; 2. Ransomware; 3. Loss or Theft of Equipment or Data; 4. Insider Accidental or Malicious Data Loss; 5. Attacks Against Network Connected Medical Devices.

The top ten cybersecurity practices: 1. Email Protection Systems; 2. Endpoint Protection Systems; 3. Access Management; 4. Data Protection and Loss Prevention; 5. Asset Management; 6. Network Management; 7. Vulnerability Management; 8. Incident Response; 9. Network Connected Medical Device Security; 10. Cybersecurity Oversight and Governance.

NYC DOH will incorporate these top threats and practices into their cybersecurity prevention and mitigation efforts. This will be accomplished by reviewing the current cybersecurity infrastructure of NYC DOH, reviewing previous cyber-attacks against health systems, making improvements in areas in which there is vulnerability and strengthening redundancies to improve overall system strength. Incident response systems will run through simulations and practice responding to different attacks and test coordination and resilience efforts in prevention and response.

Coordination with the New York City Emergency Management team, the New York City Office of Technology and Innovation, the Mayor's Office, NYDP, FBI, DHS and others as indicated may be necessary to develop a response plan and to assess the scope of the cyber-attack, the vulnerability of the systems and databases, and operational disruptions that may be necessary in order to bring services back online and accessible to members of the public.

Matching Available Resources To The Needs

Conducting a thorough assessment and cataloging of all available resources allows the NYC Department of Health to quickly identify what is on hand and what might be needed during a cyber-attack. This process is foundational for rapid resource mobilization and effective response. Specifically, establishing a comprehensive asset inventory provides visibility over the core assets, such as endpoints, cloud workloads, applications, and accounts. This can help to identify security gaps and to prioritize the protection of high-value items.[15] Additionally, developing a consistent risk assessment framework such as the MITRE ATT&CK framework, the cyber kill chain, and the National Vulnerability Database (NVD) can regularly evaluate the vulnerabilities of the system.[15] Documenting local caches and planning for backup systems for key resources management ensures continuity of main operations during an attack. Also, regular updates, training, and drills can maintain the preparedness of the health system and adapt quickly to new threats. This proactive approach can minimize the impact of cyber attacks and ensure the continuity of primary healthcare operations.

Meanwhile, establishing partnerships with neighboring health departments and private sector partners can ensure a rapid and coordinated response during a cyber attack by providing cybersecurity tools, technical support, and emergency services. Specifically, key private sectors include technology firms such as Palo Alto Networks, CrowdStrike, and FireEye, which provide advanced cybersecurity solutions and threat prevention services.[16,17,18] Moreover, Public-private partnership initiatives such as those led by the New York City Economic Development Corporation (NYCEDC) and NYC Cyber Command (NYC3) can enhance the city's cyber defenses.[19,20] Also, collaboration with the FBI through programs like the Domestic Security Alliance Council (DSAC) and InfraGard, as well as the Joint Security Operations Center (JSOC) in NYC, can further bolster real-time response capabilities and ensure comprehensive protection against cyber threats.[21]

The NYC Department of Health can prioritize surveillance and the identification of cyber threats to ensure rapid detection and response. Through appropriate staff preparedness/training, non-essential programs can temporarily suspend to reallocate staff to urgent areas for maintaining the overall functions. Clear communication policies can establish a hierarchy and streamline decision-making process. Also, detailed and regularly updated Standard Operating Procedures (SOPs) can provide a consistent response framework.[22] Meanwhile, Multiple communication channels such as emergency notifications can ensure timely information spreading. Regular training sessions and awareness campaigns can also keep staff informed to feedback mechanisms, such as two-way communication and post-incident reviews, which can help improve responses. Lastly, maintaining transparency and consistent messaging builds trust and prevents misinformation, ensuring an effective and coordinated response to cyber-attacks.

Implementing Strategies To Reduce The Health Impacts / Evaluating The Effectiveness Of Disaster Response

Disaster response to a cyberattack by NYC DOH is an area where there is much room for improvement with continuous evaluation. Managing all-hazards risks to critical infrastructure in the HPH Sector requires a comprehensive and integrated approach to:

-Identify Risks • Identify and prepare for a range of potential threats and hazards.

-Reduce Vulnerabilities • Reduce the vulnerabilities of identified critical assets, systems, and networks, including those associated with critical internal and out-of-sector dependencies and interdependencies.

-Mitigate Impacts • Mitigate the potential impacts to critical infrastructure and enable the timely restoration of functionality when events and incidents do occur.

-Enhance Resilience • Adapt to changing conditions to withstand and rapidly recover from disruption due to emergencies, irrespective of the cause of the disruption (manmade or natural).

First, clear evaluation criteria should be set out, which should focus on the response and restoration times of IT systems and, most importantly, the effectiveness of communication—especially with populations of non-English-speaking elderly individuals. Key performance indicators (KPIs) should include the time taken from when the incident was identified and corrective actions were executed, the rate at which the communication occurred internally and between external bodies, and how effective the practical care of the patient was during the attack. It can be done by gathering incident logs alongside the communication records, plus the information from the feedback of the affected parties to show them where the issue is.[24]

Continuous monitoring during a cyberattack is of the essence so that, if necessary, the impact of remediation can be wielded with constant reevaluation of the real-time situation. This consists of informing the public with regular updates, viewing the system's performance through dashboards, and providing open communication with the operations. It is, therefore, essential to deliver significant, easily understandable information to non-English-speaking elderly populations quickly. Indeed, extended communication through multilingual alerts and community liaisons has been demonstrated to increase communication with at-risk populations significantly. Direct communication through text alerts can ensure critical information is in the hands of the people faster than ever before.[25] In addition to communication with vulnerable populations, the effectiveness of staff communication has to be established so that they can be prepared and respond appropriately throughout the incident. The activities evaluation will apply to all group members to ensure that both vulnerable populations and staff are covered. Staff training and readiness must be accessed for response time and coordination in dealing with cyber incidents continuously. Staff feedback will be critical to the effectiveness of such communications and response protocols in providing continued improvement. This helps ensure that all the personnel are knowledgeable and informed when dealing with the incident.

Furthermore, a full after-action review (AAR) helps learn from the response efforts. This is documented to involve debriefing sessions with all parties, the documentation of what worked and what did not, and an after-action report that would consolidate all the recommendations for improvement. The PIO has a primary responsibility for the management and accuracy of the diffusion of the information during and after the incident. He would want to put lessons learned into better protocols and training programs.[26] Regular drills and exercises will test the enhancements so that NYC DOH is more prepared for future cyber threats. It would involve a set interval in a feedback loop through receiving feedback from staff, stakeholders, and the affected community. It would analyze such information to deduce the trends and areas of improvement of the response plan and make the necessary modifications. By such constant repetition of the process, the department will improve at ensuring the protection of all New Yorkers and, above all, the vulnerable non-English-speaking elderly population.[27]

References

1. Gentes-Hunt, L. (2021, July 15). Cyberattack exposes protected health information of 43K New Yorkers. HealthITSecurity. Retrieved from https://healthitsecurity.com/news/cyberattack-exposes-protected-health-information-of-43k-new-yorkers

2. Landi, H. (2019, November 6). Ransomware attack at Brooklyn Hospital Center results in permanent loss of some patient data. FierceHealthcare. Retrieved from https://www.fiercehealthcare.com/tech/ransomware-attack-at-brooklyn-hospital-center-results-permanent-loss-some-patient-data

3. The NYC Health Department's Strategic Plan. nyc.gov. Published February 2024. Accessed June 2, 2024. https://www.nyc.gov/assets/doh/downloads/pdf/about/strategic-plan-mission-vision-values.pdf

4. How to Send Mass Text Alerts in an Emergency. Twilio. Accessed June 3, 2024. https://www.twilio.com/en-us/blog/emergency-mass-text-alerts

5. Critical Communications Solutions and Platform. OnSolve. Accessed June 3, 2024. https://www.onsolve.com/platform-products/critical-communications/

6. MailJerry. ProtonMail vs Tutanota: Which Secure Email Provider Wins 2024? MailJerry Email Migration Tool. Published February 14, 2024. Accessed June 3, 2024. https://www.mailjerry.com/protonmail-vs-tutanota/

7. Timofeeva D. Secure Email Showdown: Tutanota vs. ProtonMail. ForestVPN. Published February 29, 2024. Accessed June 3, 2024. https://forestvpn.com/blog/guide/secure-email-tutanota-protonmail/

8. Crisis Communications and the Role of the PIO. www.iafc.org. https://www.iafc.org/blogs/blog/iafc/2019/12/12/crisis-communications-and-the-role-of-the-pio

9. Emergency Preparedness Exercise - NYC Health. www.nyc.gov. Accessed June 3, 2024. https://www.nyc.gov/site/doh/about/press/pr2019/emergency-preparedness-exercise-in-hospitals-and-nursing-homes.page

10. NYP.org - NewYork-Presbyterian. www.nyp.org. https://www.nyp.org/

11. Mount Sinai. Mount Sinai Health System. Mount Sinai Health System. Published 2019. https://www.mountsinai.org/

12. Fema.gov. Published 2017. https://emilms.fema.gov/is_0200c/groups/84.html

13. Healthcare System Cybersecurity. HHS.Gov. Published February 2021, revised October 2022. https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf

14. What's New in the HICP 2023 Edition. HHS.Gov. Retrieved June 22, 2024. https://405d.hhs.gov/Documents/405d-hicp-highlight.pdf

15. Healthcare System Cybersecurity. HHS.Gov. Published February 2021, revised October 2022. https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf

16. How to Break the Cyber Attack Lifecycle - Palo Alto Networks. www.paloaltonetworks.com. Accessed June 10, 2024. https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

17. CrowdStrike: Stop breaches. Drive business. CrowdStrike.com. Accessed June 10, 2024. https://www.crowdstrike.com/en-us/?utm_campaign=brand&utm_content=crwd-brand-amer-us-en-psp-x-trl-x-tct-x_x_x_core-x&utm_medium=sem&utm_source=goog&utm_term=crowdstrike&cq_cmp=19616633032&cq_plac=&gad_source=1&gclid=EAIaIQobChMI4fa

18. About FireEye. Fireeye.dev. Accessed June 10, 2024. https://fireeye.dev/docs/about/fireeye/

19. Choose NYC | Grow Your Business in NYC. choose.nyc. Accessed June 10, 2024. https://choose.nyc/?utm_source=multiview&utm_medium=search&utm_campaign=fy24bizdev&gad_source=1&gclid=EAIaIQobChMI-5rUxo7ShgMV7VtHAR1H0QVzEAAYASAAEgJSZ_D_BwE&gclsrc=aw.ds

20. NYC Office of Technology and Innovation - OTI. www.nyc.gov. Accessed June 10, 2024. https://www.nyc.gov/content/oti/pages/meet-the-team/cyber-command

21. Mayor Adams Unveils Joint Security Operations Center to Combat Cybersecurity Attacks. The official website of the City of New York. Published February 22, 2022. Accessed June 10, 2024. https://www.nyc.gov/office-of-the-mayor/news/088-22/mayor-adams-governor-hochul-joint-security-operations-center-combat-cybersecurity#/0

22. Cyber Incident Response. New York Office of Information Technology Services. Updated November 3, 2023. Accessed June 10, 2024. https://its.ny.gov/system/files/documents/2023/11/nys-s13-005-cyber-incident-response_0.pdf

23. NYC Office of Technology and Innovation - OTI. www.nyc.gov. Accessed June 10, 2024. https://www.nyc.gov/content/oti/pages/meet-the-team/cyber-command

24. Mayor Adams Unveils Joint Security Operations Center to Combat Cybersecurity Attacks. The official website of the City of New York. Published February 22, 2022. Accessed June 10, 2024. https://www.nyc.gov/office-of-the-mayor/news/088-22/mayor-adams-governor-hochul-joint-security-operations-center-combat-cybersecurity#/0

25. Cyber Incident Response. New York Office of Information Technology Services. Updated November 3, 2023. Accessed June 10, 2024. https://its.ny.gov/system/files/documents/2023/11/nys-s13-005-cyber-incident-response_0.pdf

26. IAFC.Crisis communications and the role of the PIO. Published December 12 2019. Accessed June 10, 2024. https://www.iafc.org/blogs/blog/iafc/2019/12/12/crisis-communications-and-the-role-of-the-pio

27. NYC Department of Health. The NYC Health Department's strategic plan. Published February 2024. Accessed June 10, 2024. https://www.nyc.gov/assets/doh/downloads/pdf/about/strategic-plan-mission-vision-values.pdf

Annex I: Threat and Hazards Assessment Table - New York City Department of Health, NY

Natural	Technological	Human-caused
Resulting from acts of nature	Involves accidents or the failures of systems and structures	Caused by the intentional actions of an adversary
·Flooding events – As a result of heavy rainfall, several areas of the city are prone to flooding events, particularly along the southern parts of Brooklyn and Queens. In 2023 intensified rainfall resulted in flooding in subways, throughout streets and in the lower floors/basements of residential areas. · Earthquakes – Though not common, a recent 4.8 magnitude earthquake in New Jersey resulted in shocks being felt throughout NYC. · Unsafe air quality - Canadian wildfires in 2023 resulted in days of unsafe air quality in NYC, which are expected to continue in 2024. Even those confined to indoor spaces were directed to use air filters to keep the air inside safe to breathe. ·Hurricanes – Tropical storms have made landfall within NYC and caused massive amounts of flooding, property damage and disruptions to transportation and other services.	· Cyber insecurity – With so many different departments, software applications and systems used throughout NYC, it is imperative that these systems do not inadvertently expose sensitive information on networks accessible by the public or other unauthorized actors. · Bridges and Tunnels – There are hundreds of bridges and tunnels throughout NYC; an accident or breakdown in any single structure could wreak havoc on the city and cause death and injuries to many. · Public Utilities – A blackout in the summer of 1977 caused mayhem in the city, while a similar blackout in 2003 resulted in mostly inconvenience. With our society ever more reliant on power to connect to systems and services, having backup systems in place and being able to respond to utility failure is critical. · IT Networks/Systems – Many systems connect to services via the internet and a rupture of this kind could result in massive disruptions to facilities attempting to record/review/access patient data.	· Acts of terrorism – As the largest city in the United States and home of the world's finance and banking areas, NYC has long been a target for terrorist attacks. Multiple attacks on the World Trade Center and other attempted bombings have resulted in the deaths and injuries of thoughts of people. · Mass Shootings – In 2022 a mass shooting event occurred on a subway train in Brooklyn. While NYC has among the strictest gun laws in the country, there have been other shooting events targeting police and civilians over the years. · Biological/chemical attacks – Whether it's the still-debated origins of Covid-19 and other possible lab-developed agents or the anthrax mailers sent to various entities in NYC, the city is a target for such forms of attack · Cyber-attacks – Cyber-attacks against NYC entities have been ongoing with attacks having targeted health facilities, public schools, law departments, airports and private companies. Such attacks can cost millions to recover from and release individual's private information.

Annex II: Drills and Exercise **Training Seminar: “**Only You Can Prevent Cyber-Attacks” Cyber-Attack on New York City Department of Health	
Objectives of your Training Seminar (What mitigation strategy are you advocating?)	To help staff at the New York City Department of Health (NYC DOH) understand ways in which they can play a role in preventing cyber-attacks by sticking with best practices
Estimate Length of Training	All staff will attend in-person training and then annually thereafter attend virtually through video lectures. Estimated time of in-person training will be 2 hours and video lectures will be 1 hour
Target Audience and max size of audience.	All of the health department staff, interns and any other contractors with access to NYCDOH databases. Max in-person audience will be 100 attendees
Who would be a good candidate (e.g., structural engineer, health dept. official, first responder?) as Facilitator of this session? Why?	Implemented by Chief Information Security Officer, Cyber Command from the NYC Office of Technology and Innovation (NYC OTI) and NYC DOH Chief Information Officer for Information Technology. These staff are trained in recognizing the ways in which many users at organizations may be susceptible to cyber-attacks (phishing, malware, etc.) which can lead to larger attacks on the system and best practices for users to engage in to prevent actions which may result in being compromised.

What do you want community members to do as a result of their attending this session?	1. Staff to recognize ways in which they can prevent cyber-attacks with their own actions. 2. Clicking links in emails, opening attachments in emails sent from outside entities, giving out personal information or sharing passwords will be remembered as prohibited activities for department staff 3. Staff to be vigilant about protecting themselves while on NYC DOH devices and web pages, including verifying the identities of individuals by contacting them if there is any uncertainty about who they are engaging with. 4. Collective efforts and education of cyber security will permeate throughout the culture of the NYC DOH which will encourage staff to have a high awareness of their activities and the activities of others which may help maintain safety of the system.
Strategies to increase community uptake of your mitigation (We have lots of useful links for checklists on the Course Home page under the Important Links page.) List the ones you think might be useful (in the appropriate language) or provide a title or two of a list or handout that you think would be good to give out to attendees.	1. Email blasts to all NYC DOH users on new types of cyber threats and ways users can maintain cyber safety 2. Distribution of educational materials regarding cyber safety 3. Incorporating real life events and stories of individuals and organizations that have been subject to cyber-attacks and what those burdens are for those who have been attacked 4. Providing posters to be hung up on offices throughout the NYC DOH with information about cyber safety