NACCHO[SM]
National Association of County & City Health Officials

[FACT SHEET]

October 2024

Local Health Departments: Instrumental Partners in Cybersecurity Preparedness

This updated fact sheet is part of an ongoing effort by the National Association of County and City Health Officials (NACCHO) to ensure local health departments (LHDs) have access to tools and resources to implement effective cyber-hygiene and cybersecurity preparedness strategies.

The Need

Cyber-related disruptions are on the rise and remain an ever-growing threat, with the Healthcare and Public Health (HPH) sector experiencing a 42% increase in ransomware attacks in 2022 compared to 2021. These disruptions can include impacts on the collection and analysis of epidemiological data, supply chain of medical countermeasures, distribution of emergency supplies, and more. According to NACCHO's *2022 Preparedness Profile*, 48% of the local health departments feel very concerned about the impact of a cyber-related attack and 26% feel not at all prepared, whereas only 13% feel very prepared.

How to Use This Fact Sheet

There are strategies and tactics that can be utilized by local health departments and leaders alike to mitigate and prepare for a cyber-attack or disruption. This fact sheet explores some of those strategies and tactics. Local health department leaders and preparedness staff are encouraged to partner with their IT counterparts to identify, prepare for, and mitigate potential cybersecurity disruptions.

Dangers of Cybersecurity Disruptions

Threats can take the form of malware that compromise system performance and integrity, updates that don't apply to out-of-date devices, ransomware that can hold important information ransom by bad actors, and careless or malicious insiders who can steal, release, or destroy information. With increased use of and reliance on technology, threats to cybersecurity present a growing and serious challenge for the public and private sectors.

Public health and healthcare organizations are attractive targets for cyber threats as they collect sensitive personal health data, payment information, and impacts to their services will garner much public attention. For example, in early 2024, cybercriminals broke into an unsecured computer server used by Change Healthcare, a large insurance billing company that processes about 15 billion health care transactions annually. This incident highlighted the vulnerability of the Healthcare and Public Health sector along with the need for a collaborative strengthening of cyber resiliency, training, and preparedness measures.

Local Health Department Role in a Cyber Disruption

Staff and leaders from across health departments play a critical role in preparing for and responding to a cyber disruption. NACCHO's *2022 National Profile*, found that more than half of LHDs perform their own data management, software selection, and IT hardware budget allocation or acquisition. However, city or county IT, along with some state health departments, are involved in data management for LHDs. This emphasizes the need for cross collaboration in planning efforts.

Maintaining a strong cybersecurity infrastructure is essential for the vital work conducted each day by local health departments of all sizes—from rural to urban. Responding health department preparedness staff generally performed the following cybersecurity preparedness roles:

- Sending notifications to partners and the community.
- Developing internal and external contingency plans.
- Assessing infrastructure and service impacts.
- Convening or collaborating with healthcare coalition (HCC) partners.
- Participating in Emergency Operation Center activations.
- Providing situational updates to partners and the public.
- Collaborating with internal or external IT partners to plan for a cyber-related disruption or attack.

[FACT SHEET]

October 2024

Planning Considerations: Action Items for Increased Cybersecurity

Cybersecurity Preparedness Planning

To follow are some of the current tactics used by state and local preparedness representatives in cybersecurity preparedness planning. These are items for local health department preparedness staff to consider as they plan with their IT counterparts.

Establish Access Requirements and Specifications to Ensure Data is Secure

- ☐ Require encrypted access cards or multi-factor authentication to use computers.
- ☐ Restrict the use of flash drives on agency computers.
- ☐ Control physical facility access and log all facility visitors.
- ☐ Establish and enforce password policies including password age, minimum length, and complexity.
- ☐ Implement computer-use, internet, and e-mail policies.
- ☐ Enable e-mail and password encryption.
- ☐ Establish and enforce mobile and smart device security policies and solutions.
- ☐ Activate computer auto-lock and timeout settings.
- ☐ Set up safeguards to stop outside electronics from accessing agency-provided devices including laptops and mobile devices.
- ☐ Deploy next generation firewalls, threat detection, and prevention systems that limit access to dangerous sites.

Assess Systems to Identify Vulnerabilities

- ☐ Conduct user testing on e-mail and phone systems to look for vulnerabilities.
- ☐ Perform periodic network and application assessments using vulnerability assessment technologies and software.
- ☐ Partner with the Cybersecurity & Infrastructure Security Agency (CISA) for vulnerability assessments.
- ☐ Evaluate new software for cyber issues.

Establish Redundant Systems as a Failsafe

- ☐ Store data, partner contacts, and applications on a secure cloud environment.
- ☐ Establish disaster recovery site and test site procedures regularly.
- ☐ Back up organizational data regularly, print hard copies of operational plans and test recovery procedures.

Train Employees

- ☐ Develop the workforce capacity needed to prioritize and ensure cybersecurity awareness and technical capabilities.
- ☐ Offer online training on cybersecurity and mandate annual training for all employees.
- ☐ Conduct annual HIPAA computer security awareness training.
- ☐ Conduct annual training on cybersecurity and IT topics.
- ☐ Conduct email phishing training and tests for all employees.
- ☐ Identify personnel to be trained in ham radio operations for disaster response.

Strengthen Employee Cybersecurity Awareness

- ☐ Send employees regular notices for IT maintenance.
- ☐ Send out monthly messages on IT topics.

Conduct Preparedness Activities

- ☐ Develop and regularly test a disaster recovery plan and cyber incident response plan.
- ☐ Establish a cybersecurity taskforce.
- ☐ Conduct an e-mail phishing drill with all employees to educate them on cyber threats.

[FACT SHEET]

October 2024

Cybersecurity Response Considerations

While there are many potential actions that health departments can take in the aftermath of cyber disruption, impacted individuals should immediately notify law enforcement in the event of a ransomware event, and/or IT department representatives to make them aware of the attack or disruption. Additional actions health departments may take following a cyber disruption include the following:

- Identify impacts to patient care and services.
- Compare information to other sources for patient identification.
- Implement and test continuity of operations plans.
- Perform regular system functionality checks.
- Preserve network, server, and application security logs; establish automated security log management tools and reviewing logs for abnormal activities.
- Follow disclosure protocols (HIPAA notification, etc.).
- Implement a notification and disconnect plan.
- Notify those affected regarding what information was stolen.

Following a cyber disruption or attack, jurisdictional partners and the public will have a variety of information needs related to health department operations. Potential items for which health departments should consider developing communications strategies include:

Audience - Response Partners and Health Department Staff

- Source and impact of the incident
- Continuity of operations instructions
- Timeline for the response
- Health department personnel concerns
- Control of sensitive information versus transparency

Audience - Response Partners, Health Department Staff, and the Public

- Information on services impacted
- Provision of regular updates

Potential Barriers

Some health departments have encountered barriers in the process of building their cybersecurity preparedness capabilities. Below is a listing of identified barriers and potential solutions.

Barrier	Potential Solutions
Difficult to get leadership buy-in	Educate leadership on potential threats and costs of attack.
Cybersecurity is not a priority	Perform an assessment of cybersecurity vulnerabilities and articulate the risks of the threats.
Limited understanding of cyber threats and safeguards	Offer cybersecurity training.
Limited money and resources to invest in IT	Identify low-cost cybersecurity strategies. Articulate the return on investment and costs of a breach. Utilize resources from CISA to conduct vulnerability assessments or for Continuity of Operations (COOP) planning.
Mandatory use of legacy systems	Work with IT to determine vulnerabilities of the system and develop migration strategies.
Discussions on cybersecurity rarely advance to planning phase	Set planning goals and identify next steps after each meeting.
Disconnect between health department preparedness staff and IT staff	Engage local and state IT department and cyber teams in healthcare solution planning.

Resources

Below is a listing of resources for cybersecurity preparedness:

- CISA Resources and Tools
- HHS Cybersecurity Gateway, a one-stop shop for all things HPH Cybersecurity Strategic Plans and Actions
- Healthcare and Public Health Cybersecurity Performance Goals, HHS U.S. Department of Homeland Security Resources
- ASPR TRACIE Cybersecurity Topic Collection
- Health Industry Cybersecurity - Strategic Plan 2024-2029, Health Sector Coordinating Council Cybersecurity Working Group
- ASPR Strategic Plan 2022-2026 Goal 1

[FACT SHEET]

October 2024

Next Steps

This fact sheet can serve as a guide to navigate the tactics, strategies, and resources that support the public health sector in strengthening their cyber hygiene. With a heavy reliance on technology, public health preparedness staff, local and state IT staff, and public health leaders can play a role in strengthening resilience to cyber disruptions within their communities.

The National Security Memorandum 22 released in April 2024 empowers the Department of Homeland Security to lead the federal government's effort to secure our nation's critical infrastructure alongside CISA. The U.S. Department of Health and Human Services leads the way in establishing and implementing the cybersecurity performance goals (CPGs) for the Healthcare and Public Health sector. LHDs can tap into these resources, and opportunities such as conducting vulnerability assessments through CISA, to align efforts with the CPGs. Increased collaboration between IT, healthcare, and public health will lead to a more unified effort in safeguarding the nation from cyber-related disruptions and threats. NACCHO echoes this need for cybersecurity resilience, and advocates for an increase in cybersecurity preparedness for all local health departments.

Acknowledgments

This fact sheet was supported by the Administration for Strategic Preparedness and Response (ASPR). NACCHO is grateful for this support. The contents do not necessarily represent the official views of the ASPR.

FOR MORE INFORMATION, PLEASE CONTACT:

NACCHO Preparedness Team
preparedness@naccho.org

NACCHO
National Association of County & City Health Officials

Public Health
Prevent. Promote. Protect.

The mission of the National Association of County and City Health Officials (NACCHO) is to improve the health of communities by strengthening and advocating for local health departments.

1201 Eye Street, NW, Fourth Floor • Washington, DC 20005

Phone: 202-783-5550 • Fax: 202-783-1583

www.naccho.org