NACCHO
National Association of County & City Health Officials
The National Connection for Local Public Health

[FACT SHEET]
October 2018

Cybersecurity Preparedness Considerations for Public Health and Healthcare Organizations

Background on Cybersecurity

Cyber threats have the potential to cripple public health and healthcare infrastructure and services. Threats can take the form of malware that compromise system performance and integrity, 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. Recent attacks in 2017 such as the WannaCry ransomware attack in the United Kingdom and a ransomware attack targeting local jurisdictional systems in North Carolina demonstrate that these threats are real. Many public health organizations are in only the early stages of addressing cybersecurity incident preparedness and response and need to double their efforts to further advance cybersecurity practices nationwide. This fact sheet provides information on roles, strategies, considerations, and barriers for public health and healthcare cybersecurity preparedness.

Needs Assessment Project Information

To better understand the cybersecurity preparedness needs of public health and healthcare organizations, the Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Responses (ASPR), in coordination with NACCHO, conducted a needs assessment project centered on cybersecurity preparedness. The needs assessment focused on two main topic areas: (1) cybersecurity preparedness strategies for public health and healthcare IT systems; and (2) cybersecurity incident recovery and information-sharing needs. The needs assessment questions were integrated into two sessions at the 2018 Preparedness Summit and a combination of qualitative and quantitative data was collected from conference attendees. NACCHO used the findings of the needs assessment to develop this fact sheet.

Health Department Roles

Health department staff can play a critical role in preparing for and responding to a cybersecurity attack that affects their organization's systems and operations. Responding health department preparedness staff generally performed the following cybersecurity preparedness roles:

- Sending notifications to partners and the community;
- Developing contingency plans;
- Assessing infrastructure and service impacts;
- Convening partners;
- Participating in emergency operations center operations; and
- Providing situational updates to partners and the public.

Operationalizing Cybersecurity Preparedness

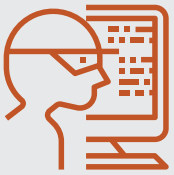
State and local preparedness representatives discussed a variety of strategies they are currently using to protect against and prepare for cyber-attacks. The strategies include the following:

The Health Department Role in Cybersecurity

Sending notifications to partners and the community

Developing contingency plans

Assessing infrastucture and service impacts



Participating in emergency operations center operations

Providing situational updates to partners and the public

Access Requirements and Specifications

- Require encrypted access cards and 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.

System Assessments

- 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.
- Hire a security consultant to assess vulnerabilities.
- Evaluate new software for cyber issues.

Redundant Systems

- Store data and applications on secure cloud environment.
- Establish disaster recovery site and test site procedures regularly.
- Back up organizational data regularly and tests recovery procedures.

Training

- 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 of cybersecurity and IT topics.

Employee Outreach

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

Preparedness Actions

- 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.

Cybersecurity Response Considerations

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

- Compare information to other sources for patient identification.
- Implement and testing of 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-attack, jurisdictional partners and the public will have a variety of information needs related to health department operations. Some potential items health departments should consider developing communications strategies for include the following:

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 what services are 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 barrier 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
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 staff and IT staff	Engage IT department and cyber teams in healthcare solution planning

Resources

Below is a listing of resources for cybersecurity preparedness:

- Cybersecurity: Risk and Recommendations for Increasingly Connected Local Health Departments (NACCHO publication)
- Troubling Gap: Why Cybersecurity Matters to Public Health Emergency Response (Preparedness Summit video)
- U.S. Department of Homeland Security Resources
- ASPR TRACIE Cybersecurity Topic Collection
- National Health - Information Sharing and Analysis Center (NH-ISAC)
- Health Care Industry Cybersecurity Task Force Website
- International City/County Management Association Cybersecurity Resources

[FACT SHEET]

October 2018

Implications and Next Steps

One overarching theme identified during the needs assessment was a need for more information from federal partners on what resources they could provide in a cyber-attack. In addition, many participants were interested in developing cybersecurity plans and expressed a need for more cybersecurity planning guidance, training, templates, and resources specifically for a public health audience. Needs assessment participants also requested tools that solicit leadership buy-in to pursue cyber planning, pre-developed message templates, and planning and exercise templates to address some of their stated barriers. NACCHO plans to work with ASPR in the future to increase awareness on existing cybersecurity resources and develop resources that address the needs of local public health planners seeking to advance their cybersecurity preparedness efforts.

Acknowledgments

This fact sheet was supported by 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
The National Connection for Local Public Health

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