A Primer on Local Public Health Cybersecurity

Justin Snair, MPA
Founder and Managing Consultant
SGNL Solutions

You are a director of a local public health department. Your county government recently completed a long process of updating and integrating its computer systems for all departments, including the health department. The update integrates mobile and medical devices, servers, and workstations and enables computer-controlled building automation technology to regulate heating and cooling, lighting systems, door locks, alarms, and refrigeration units in all county facilities. Personnel have access to networked desktop and laptop computers, voice over IP (VOIP) landlines, mobile phones and email, an electronic reporting system for vaccines administration, and an electronic vendor supply procurement system.

The United States is several months into a moderate to severe influenza season. To protect the public's health and reduce the spread of the virus, your local health department is providing free/low-cost influenza vaccine at several locations across the county from November through January. Your health department is also one year into a chronic disease and environmental monitoring research project funded by a Federal agency and a private technology firm. The research data for this project are stored on your county government's computer system.

You receive word that staff setting up a flu vaccine clinic are having trouble connecting to the electronic medical record system on the county computer network. VOIP phones services are routinely unavailable throughout the day. You receive word from your research staff that data are no longer accessible. You learn that many of the county computers, including tax payments, birth and death certificates, and county sewer and water, are locked with a ransomware message; demanding a $23,000 payment in Bitcoins to unlock the computers.

There has been news of a new computer worm – a program that infects a computer, blocks access by encrypting key components, and demands a ransom be paid for the restriction to be removed – spreading across the internet through networks and removable drives, downloading files and stealing information. Fearing that these disruptions could be due to such a worm, the county's IT department disables county-wide email services to prevent further spreading. You consider activating your health department's emergency response plan, but are uncertain if cyber-attack requires such a response. Your county emergency manager and executive leadership call a department head meeting to discuss what to do and decide to not pay the ransom.

It has been nearly two weeks since the attack began and your IT department is slowly restoring services, albeit with significant loss of data. The public is also experiencing the impacts of the cyber-attack firsthand, with excessive wait times for health department services and the

cancelling of the county flu vaccine clinics. After hearing about the cyber-attack on the news, many citizens are calling the health department to find out if their personally identifiable information and protected health information is secure and what the government is doing about the situation. To update the public about the attack, a town hall meeting is held, and you consult with your community leadership and general counsel about what information to share. It was later learned that an infected USB drive, obtained from a public health preparedness conference as a giveaway, was the culprit.

Stories of cyber criminals attacking entire local and county government systems have become more and more common in the past year. Recent events include a cyberattack in Dallas that managed to set off all 156 emergency alarms in the city, a ransomware attack in Mecklenburg County that slowed the county government to a crawl, and another in Atlanta that knocked out critical systems, forcing many city workers to revert to paper. Local and county public health departments have come to rely more heavily on technology for performing essential services, such as disease surveillance, outbreak prevention, research, and emergency response. These recent cybersecurity incidents provide a rationale for including cyber events in all-hazards planning. To mitigate or respond to this potential threat to public health, the following questions must be answered.

- What is the role of the health department in a dealing with a cybersecurity incident?
- What are the most critical systems at risk that could compromise public health in the event of a cyber-attack?
- If a cybersecurity incident like this happened right now could your operations continue?
- What contingency plans do you have in place for this type of event?
- With whom at the state and federal levels of government do you communicate with regarding a cyber-attack?
- Would a cyber-attack trigger the activation of your emergency response plan? Who is identified as the lead in such an event? Does your emergency operations plan include the use of an air gapped network and equipment (a physically isolated secure computer network)?
- When do you notify the public of the cyber incident and affected services and what information do you share?
- Would your community pay such a ransom? If not, are you prepared for the consequences of data loss and privacy breaches?

It is also important to understand that cybersecurity is not just a technological issue. Cyber threats to the public health system can be classified in terms of their capacity to present losses of integrity, losses of availability, losses of confidentiality, and physical destruction. Public health occupies a position of trust in a community. Cyber-attacks erode that trust and the public's confidence in government services, and can introduce legal and liability issues, given the breaches of protected patient health information.

The U.S. Public Health Sector

A public health system is commonly defined as all public, private, and voluntary entities[1] that contribute to the delivery of essential public health services within a jurisdiction. Nearly 2750 county and local governmental public health departments (LHDs) across the nation are responsible for epidemiological surveillance, disaster preparedness planning, emergency response, laboratory testing and coordination, health information exchange, health communication and outreach, community resilience building, public-private sector planning and exercising, hazard and risk assessments, and protecting all sectors from natural and manmade hazards. From a national critical infrastructure protection perspective, public health is a component of Healthcare and Public Health (HPH) sector, one of sixteen national critical infrastructure sectors deemed so vital that the failure or degradation of its systems, networks, or assets would have a severe impact on national security, safety, and health. Efforts to protect the critical infrastructure of the HPH sector is coordinated at the national level through various public and private councils and information sharing organizations. The public health sub-sector is comprised of distinctive governmental and non-governmental systems of human, infrastructure, and virtual assets responsible for the health and well-being of the nation, states, and communities. Public health is interconnected and interdependent to many other sectors, such those responsible for water/wastewater, energy, transportation, critical manufacturing, and supply chain.

What are the cyber risks to public health?

The *10 Essential Public Health Services* are the activities that a public health system should undertake to assure the health, safety, and security of the communities it serves. Table 1 describes the services performed by a local government public health workforce using cyber infrastructure and virtual systems.

Table 1. Impact of Cyber-attacks on 10 Essential Public Health Services

Essential Public Health Service	Key LHD Activity	Example of Vulnerability
Monitor health status to identify and solve community health problems	Health surveillance	Computer systems that collect and transfer data are vital for both active and passive surveillance
Diagnose and investigate health problems and health hazards in the community	Analysis of health information	Loss of access to information hinders the ability of LHDs to diagnose problems in the community
Inform, educate, and empower people about health issues	Delivery of health information	Attacks on information dissemination systems could limit the ability of LHDs to share information
Mobilize community partnerships and action to identify and solve health problems	Electronic coordination and planning	The loss of electronic communication could reduce the effectiveness of community partnerships when needed most

[1] Such as public health agencies at state and local levels, healthcare providers, public safety agencies, human service and charity organizations, education and youth development organizations, recreation and arts-related organizations, economic and philanthropic organizations, and environmental agencies and organizations

Develop policies and plans that support individual and community health efforts	Policy development	Educating policymakers on the public health effects of cyber threats to formulate better policies and planning may reduce the effects of a cyber-attack
Enforce laws and regulations that protect health and ensure safety	Gathering public health data	The loss of infrastructures could reduce the ability to communicate notifiable diseases or health violations
Link people to needed personal health services and assure the provision of health care when otherwise unavailable	Emergency response activities that provide people with necessary health services, including access to appropriate medical care	Loss of infrastructure would cause the denial of utility services needed to maintain the health of the public. Hospitals will encounter reduced capacity to provide medical care with the loss of a hospital system.
Assure competent public and personal health care workforce	Many activities, including outbreak management, emergency response, and disease tracking	The continuing loss of staff and funding make it difficult for LHDs to meet public needs. Increased strain on the system due to a cyber-attack will magnify this problem.
Evaluate effectiveness, accessibility, and quality of personal and population-based health services	Assessment of public health interventions	Evaluation of health interventions requires data storage and communication to measure progress toward goals.
Research for new insights and innovative solutions to health problems	Data collection for outbreak response research	Research during a cyber-crisis may be limited due to loss of infrastructure and records.

Adapted from Cybersecurity Threats to Public Health. Daniel J. Barnett, Tara Kirk Sell, Robert K. Lord, Curtis J. Jenkins, James W. Terbush, and Thomas A. Burke. World Medical & Health Policy, 5:1. 2013.

Lacking Public Health Cybersecurity

Several factors inhibit optimal cybersecurity across the public health system. First, the public health system is not easily described and is highly variable. The system is made of thousands of independent nodes, each providing services to the public using many different technological assets and levels of resources. Therefore, cyber security risk is not uniform and mitigation approaches need to be customized. Oftentimes, public health technological assets are covered under broader jurisdictional wide IT programs, contributing to a lack of focus on cyber threats by public health professionals. In addition to preparing against cyber security threats, communities around the nation are examining their physical security postures. The implementation of increased physical security measures and practices across local governments, to include public health departments, also add a layer of complexity as almost all of these measures have some type of cyber element. In a challenging budget environment, often the physical security programs and cyber security programs are competing for the same limited funds. Additional

efforts to further bring these two areas together and truly look at threats and risks across the enterprise will allow LHDs to maximize their limited funds. The enterprise view at the cyber-physical nexus will allow LHDs to analyze and determine true risks and determine which can be reduced and which risks need to be accepted. Second, at the national level, investments in improving HPH sector cybersecurity have largely focused on healthcare services and connected industry partners. Nearly all plans and tools produced at the national level focus on healthcare service providers – not public health departments. This omission is not surprising, as the evidence base for public health cyber risk and preparedness is not well established. Third, for many years representative organizations for public health were not adequately funded to participate in the national level HPH sector cybersecurity efforts or to produce cybersecurity materials for public health departments. The federal government has not established programmatic goals for such work or funded research by academic research institutions. Fourth, while there are Information Sharing Analysis Organizations/Centers (ISAO/ISAC), vital avenues for analysis and sharing of threat information, improving the overall cyber security posture of state, local, territory and tribal governments (e.g., Multi-state Information Sharing Analysis Centers), there is no ISAO/ISAC focusing specifically on public health cyber threats. The two existing HPH sector ISAO/ISACs, Healthcare Ready and National Health Information Sharing and Analysis Center (NH-ISAC) focus their efforts and products almost entirely on the interests of healthcare entities and adjacent stakeholders, such as those involved in the supply chain. Though the U.S. Department of Health and Human Services (HHS) awarded a grant in 2016 to the NH-ISAC the to help share information on cybersecurity and engage participation of healthcare and public health sector, very little effort appears to be focused on the cyber security concerns of LHDs. And fifth, LHDs, possibly taking cues from the federal government, academia, and their national representative organizations, dedicate very little attention to cyber security, as it is not often viewed as a priority or even considered at all.

What can be done to improve public health cyber preparedness?

Cyber-attacks against local governments are becoming a new normal, and our nation is not doing enough to prepare for and mitigate the risks to the public's health, safety, and security from such attacks. But there are signs of change. Recently, the National Association of County and City Health Officials (NACCHO), the representative organization for local public health departments, was funded by the HHS Office of the Assistant Secretary for Preparedness and Response (ASPR) to more fully participate in HPH sector cybersecurity efforts and to produce cybersecurity materials for public health departments. The 2018 Preparedness Summit's closing plenary session – *A Troubling Gap: Why Cyber Security Matters to Public Health Emergency Response* – aims to help attendees classify potential cyber threats and identify tactical strategies for responding to a cyberattack in their communities. Thought leaders are advocating for improved public health cyber security preparedness. The Cadmus Group has published several cyber related articles, such as *When Pandemic Management Meets Cybersecurity* and *Embrace the Cyber Security-Physical Security Nexus*, that help raise awareness about cyber threats to public health departments and governments. The American Public Health Association published *Public Health Increasingly Facing Cybersecurity Threats: Health field a top target for attacks*, presenting some of the risks encountered with a public health cyberattack. Cyber Georgia 2017, an annual convening of industry, academia, and government to examine cyber threats, presented the panel discussion *Cybersecurity and Public Health, Emergency Preparedness and Response*, which

examined hospital and public health department preparedness for emergencies and simultaneous denial of service attacks. SGNL Solutions and LAR Consulting developed the *Local Public Health Department Discussion Guide for Cybersecurity* and are testing the prototype with public health professionals during a workshop at the 2018 Preparedness Summit. These efforts, along with the leadership of the ASPR, demonstrate a large step towards improving public health cyber preparedness. But more can be done. Below is a list of action steps that can be taken by 4 different stakeholders involved in the public health system.

Federal Agencies

- Recognize the distinction between the healthcare and public health components within the HPH sector, the vulnerability of public health entities to cyber threats, and the unique consequences of a cyber-attack on the public health system.
- Provide resources to academic research institutions to conduct research to thoroughly understand the complex risk relationships between cybersecurity and public health.
- Use research to develop evidence-based policy and practices to address this threat.
- Fund the development of public health system cyber threat assessment tools.
- Develop future legislation and regulations that more fully account for the interactions between cybersecurity and public health.
- Advocating for and ensuring appropriate representation of public health entities on federal cyber working groups and federal cyber programs/projects.
- Establish a Public Health Information Sharing Analysis Organization/Center (ISAO/ISAC), or fund an existing ISAC, truly focused on coordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices amongst public health entities.

Academic Institutions

- Conduct new research to more thoroughly understand the cybersecurity risk of and consequences to public health.
- Work with research funders, public health practitioners, and evidence translation professionals to develop evidence-based practices and policies.
- Develop curricula to educate emerging public health professional of cyber threats and mitigation techniques.

National Public Health Representative Organizations

- Coordinate with academia on research efforts and the development of evidence-based policy/practices.
- Assist with the development and dissemination of public health sector cyber-security needs assessments tools.
- Advocate for the appropriate representation of public health equities on federal cyber working groups and federal cyber programs/projects.
- Develop communication materials to raise awareness of cyber threats to public health.
- Develop tools and resources to assist public health entities understand cyber risk and improve their preparedness to events.

State and Local Government

- Recognize and prioritize cybersecurity as a public health issue.
- Integrate public health cyber scenarios into training and exercise programs.
- Conduct cyber risk vulnerability assessments or include public health in existing assessments.
- Understand the implications of the physical/cyber nexus and foster better coordination amongst IT security, physical security, and public safety/preparedness teams.
- Develop cybersecurity specific emergency operation procedures and contingency plans.

These are not meant to be comprehensive, but as with many issues threaten public health – preparedness is a journey, not a destination. There will continually be new threats to deal with and identifying and taking small but systematic and coordinated steps is better than simply sticking our heads in the sand.