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

[ISSUE BRIEF]
February 2015

Cybersecurity: Risks and Recommendations for Increasingly Connected Local Health Departments

Introduction

With increased use of and reliance on technology, threats to cybersecurity present a growing and serious challenge for the public and private sectors. The passage of legislation such as the Health Information Technology for Economic and Clinical Health (HITECH) Act encourages expanded use of health information technology, which increases the need to protect health information and public health infrastructure and to improve resilience to cyber-attacks.

The National Association of County and City Health Officials (NACCHO) has prepared this issue brief to help local health departments (LHDs) learn more about cybersecurity, how public health information systems are vulnerable, and the damage that a cyber-attack can cause.

What are Cyberspace and Cybersecurity?

"**Cyberspace**" has been defined multiple times since its inception. One definition is "the realm of computer networks in which information is stored, shared, and communicated online." Cyberspace is a digital environment, made up of digitized data that are used and shared.[1] Physical systems, such as computers and databases that enable data exchange, are part of cyberspace, as well.[2] The users who upload and download data into a network are another essential component of cyberspace.

"**Cybersecurity**" is the "protection of cyberspace and related technologies, from records and electronic data to the physical structures and security systems."[3] When applied to healthcare, cybersecurity refers to the defensive measures and activities that prevent the exploitation or misuse of the cyber infrastructure within the health and public health sectors.[4] Cybersecurity measures are applied to medical devices, laboratory systems and networks, hospital and treatment center information systems, and public health information systems and databases.[5]

The physical systems that are controlled by computers, such as generators, medical devices, oxygen systems, and utilities, are an essential part of any cybersecurity plan.

Most people associate cybersecurity with sophisticated hackers using highly technical methods to break into secure networks. They assume that cybersecurity requires in-depth knowledge of information technology and computer science. However, cyber-attacks come in a variety of forms. Some of the most damaging data breaches result from simple human error.

In one instance, an employee at a Michigan-based company received an electronic request from what appeared to be a secure sender. The bank routinely used electronic messages to renew its digital certificates. Assuming the e-mail was

legitimate, the employee responded to the request and provided the company's online banking credentials. Within a three-hour period, the perpetrator made 47 wire transfers totaling more than $550,000 to accounts around the world.[6] This example illustrates how simple cyber-attacks, which often employ social engineering techniques, can be extremely effective in accessing protected information.

Complicated attacks affect not only computer systems but also the physical infrastructure those systems control. The Stuxnet computer worm illustrates this point. Discovered in 2010, this virus infiltrated secure networks worldwide and took control of the programmable logic controllers that control the automation of various mechanical parts. In 2010, the Stuxnet virus gained control of the system that controls Iran's nuclear centrifuges, causing the centrifuges to spin too fast, destroying them. The virus not only changed the functions of the centrifuges but also hid its actions.[7]

Whether an attack on health information systems is advanced or simple, the potential dangers to the public's health are real. The healthcare data delivery system requires Internet access and intact data storages and data-delivery systems. Emergency planners need to consider extended loss of power, telecommunications, access to data storage, and the Internet to mitigate the possible threats to their communities and the nation's health. LHDs must make cybersecurity a priority because any loss in infrastructure can severely limit their ability to track diseases or respond to disasters.

Cybersecurity Risks and Vulnerabilities

The three goals of cybersecurity are to maintain system confidentiality, integrity, and availability. System confidentiality is achieved when information is accessible only to authorized users. System integrity means that an information system will work as designed. System availability refers to a system's ability to work as needed in a timely manner. For LHDs, the failure of a critical information system could be harmful to a patient or community. For example, if someone used a laptop to tamper with a Web-enabled medical device, such as a pacemaker, the results could be deadly.

A threat is any circumstance or event with the potential to adversely affect a cyber-system system through unauthorized access, destruction, disclosure, modification of data, or denial of service. A vulnerability is an exploitable weakness in a system.[8] Sound cybersecurity requires assessing for vulnerabilities and defending these weaknesses from exploitation.

For LHDs, the failure of a critical information system could be harmful to a patient or community.

Major Threats

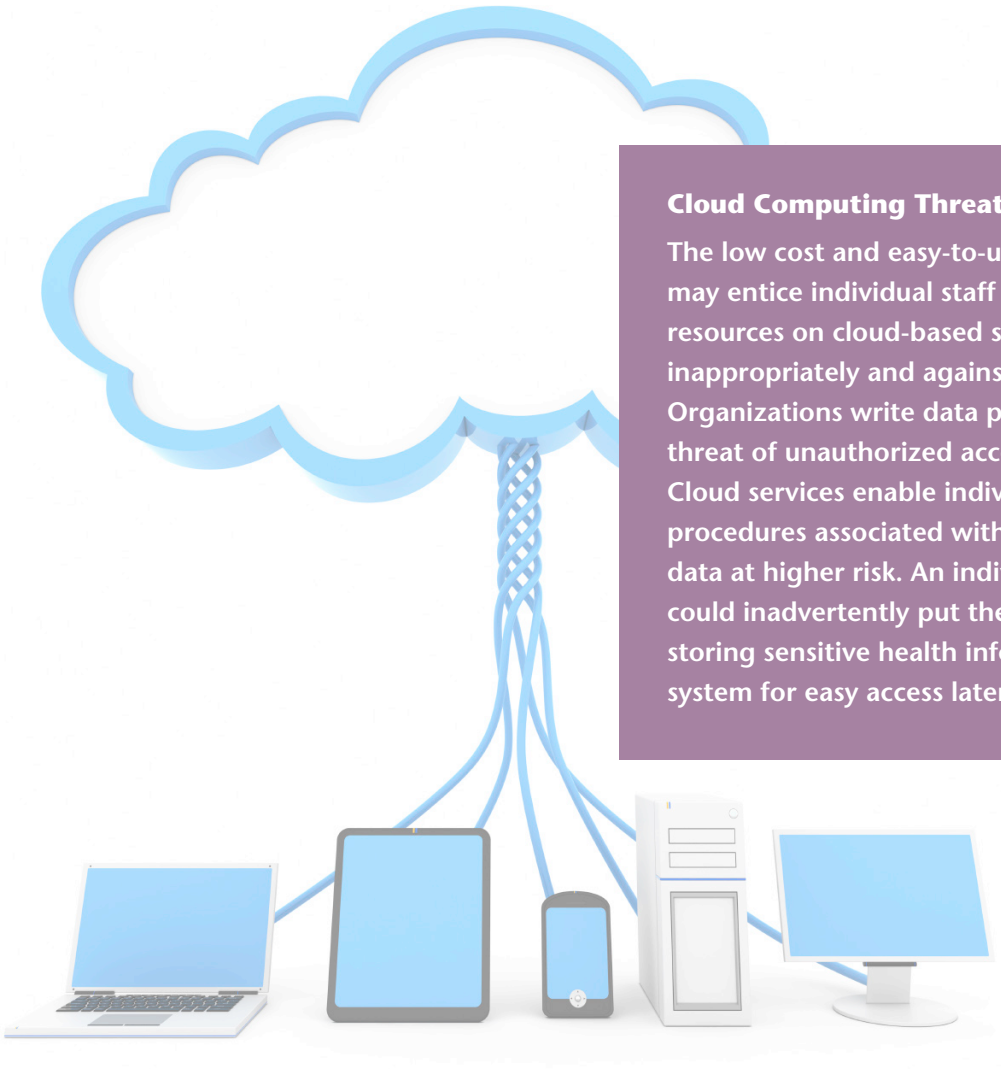
To assist critical infrastructure sectors in defending their cybersecurity systems, the Health and Public Health Sector Cybersecurity working group, part of the Department of Homeland Security's Critical Infrastructures Protection Cybersecurity Program, identified the following major threats facing the health and public health sector:[9]

- **Insider Threats:** Employees or trusted third parties can intentionally or unknowingly damage a system and steal private data. For example, staff who install an HVAC system could attempt to sabotage the infrastructure virtually. Employees could steal Social Security numbers for personal gain or destroy or delete critical files.
- **Access Control Breaches:** Malicious users may try to manipulate or bypass access control systems or procedures to gain unauthorized access to sensitive information or restricted sections of a facility.
- **Malware:** Malicious software programs can damage or do other unwanted actions to a computer system. Viruses, spyware, and Trojan horses are common types of malware.
- **Network Breaches:** An adversary can gain unauthorized access to a network and manipulate that system to perform unauthorized functions.

System Threats

Other threats seek to exploit computer system vulnerabilities such as the following:[10]

- **Lack of Antivirus Software:** Antivirus software scans a computer for any malware or malicious code. Lacking anti-malware software, the user is unaware of any computer viruses that have attacked his or her computer. According a 2013 survey by Microsoft, nearly a quarter of the organizations surveyed lacked antivirus software.
- **Lack of Intrusion Protection:** An intrusion detection system (IDS) is software that monitors network or system activities for malicious activities. Network administrators that do not use IDS have difficulty detecting unauthorized activity.
- **Inadequate Patch Management:** A patch is an update to a software's code that prevents the successful exploitation of a particular vulnerability in the code. Software patches are seldom installed on time, exposing programs to cyber-attacks.
- **Employee Access to Data:** A vulnerability is created when all staff can access information vital to an organization's operations. For example, LHD staff may need to access Social Security numbers to carry out vital work functions.



Cloud Computing Threats

The low cost and easy-to-use nature of cloud storage may entice individual staff to store information resources on cloud-based systems, perhaps inappropriately and against organizational policy. Organizations write data policies to minimize the threat of unauthorized access and the misuse of data. Cloud services enable individuals to skip the safety procedures associated with specific data, putting the data at higher risk. An individual working for an LHD could inadvertently put the department at risk by storing sensitive health information in a cloud-based system for easy access later.[11]

Health Data and the Risk of a Data Breach

Healthcare and public health patient information may be a "soft target" for cyber-attacks. Because of the healthcare industry's fragmented nature, it seems to lag behind other critical industries with respect to cyber threat mitigation plans. The Office for Civil Rights (OCR), which enforces privacy and security regulations for the Department of Health and Human Services, reported in 2014 that only 62 of more than 800 breaches of protected health information (PHI) involved cyber-attacks.[12]

Evidence suggests that many organizations are not mature enough to detect data breaches, contributing to the low level of health-related cyber-attacks that are reported.[13] Healthcare and public health organizations are susceptible to cyber-attacks for three reasons:[14]

- Security for health information systems is not prioritized;
- The high frequency of data exchange requires many open connections to a healthcare information system; and
- The healthcare and public health workforce is largely untrained in cyber security practices.

The value of health data provides a strong incentive to hackers who can illegally access patient information. Patient medical data on the black market has nearly 10 times the value of credit card data. Birth dates, billing information, and diagnosis codes, used by both healthcare providers and LHDs, are the most valuable to data hackers because they allow hackers to create fake IDs to purchase medical equipment or file false claims with insurers by combining a patient number with a false provider number.[15]

These factors make health data breaches extremely costly and very large in scale. In August 2014, Community Health Systems, one of the largest U.S. hospital groups, reported that it had been the victim of a cyber-attack from China, which resulted in the theft of Social Security numbers and other personal data belonging to 4.5 million patients. This attack was the largest of its type involving patient information since the Department of Health and Human Services started tracking such breaches in 2009.[16]

LHDs are not necessarily considered covered entities under HIPAA. However, if a public health agency provides healthcare or insures individuals for healthcare costs, the data related to these specific activities are considered covered activities under HIPAA.

A data breach that results in the unauthorized access of patient data also carries legal penalties. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), forms the bedrock of health information security in the United States.[17] Under the law, entities covered under HIPAA are responsible for data breaches, even if they did not know they were violating the law (42 USC § 1320D-5(a)(1)(A)). HIPAA carries a maximum penalty of $50,000 per violation.[18]

HIPAA established a set of national standards for the confidentiality, integrity, and availability of electronic PHI by requiring that covered entities and business associates implement reasonable and appropriate administrative, technical, and physical safeguards.[19] Such safeguards include ensuring the confidentiality, integrity, and availability of consumers' PHI and ensuring the information can be received, maintained, or transmitted. HIPAA also requires that covered entities identify and protect against reasonably anticipated threats to security and improper disclosure of PHI.[20]

Covered entities under HIPAA must perform risk assessments and risk management under the threat of punishment. The covered entity must evaluate both the risk of a data breach and its impact on the owners of the breached data. Risk management is the implementation of security measures that identify risks and the maintenance of continuous and appropriately monitored security risks.[21]

LHDs are not necessarily considered covered entities under HIPAA. However, if a public health agency provides healthcare or insures individuals for healthcare costs, the data related to these specific activities are considered covered activities under HIPAA. This does not mean all data used in the LHD must comply with HIPAA. An LHD can label itself a hybrid entity, meaning that it performs covered and non-covered data activities. This designation as a hybrid entity will require that only the covered, healthcare-related data comply formally with HIPAA.[22]

Parts of the HITECH Act update HIPAA. The HITECH Act requires entities covered by HIPAA to report data breaches that affect more than 500 people to the Department of Health and Human Services. Additionally, the HITECH Act imposes notification requirements on covered entities, business associates, vendors of personal health records, and related entities if a breach of PHI occurs.[23]

Cyber-Attacks and National Security

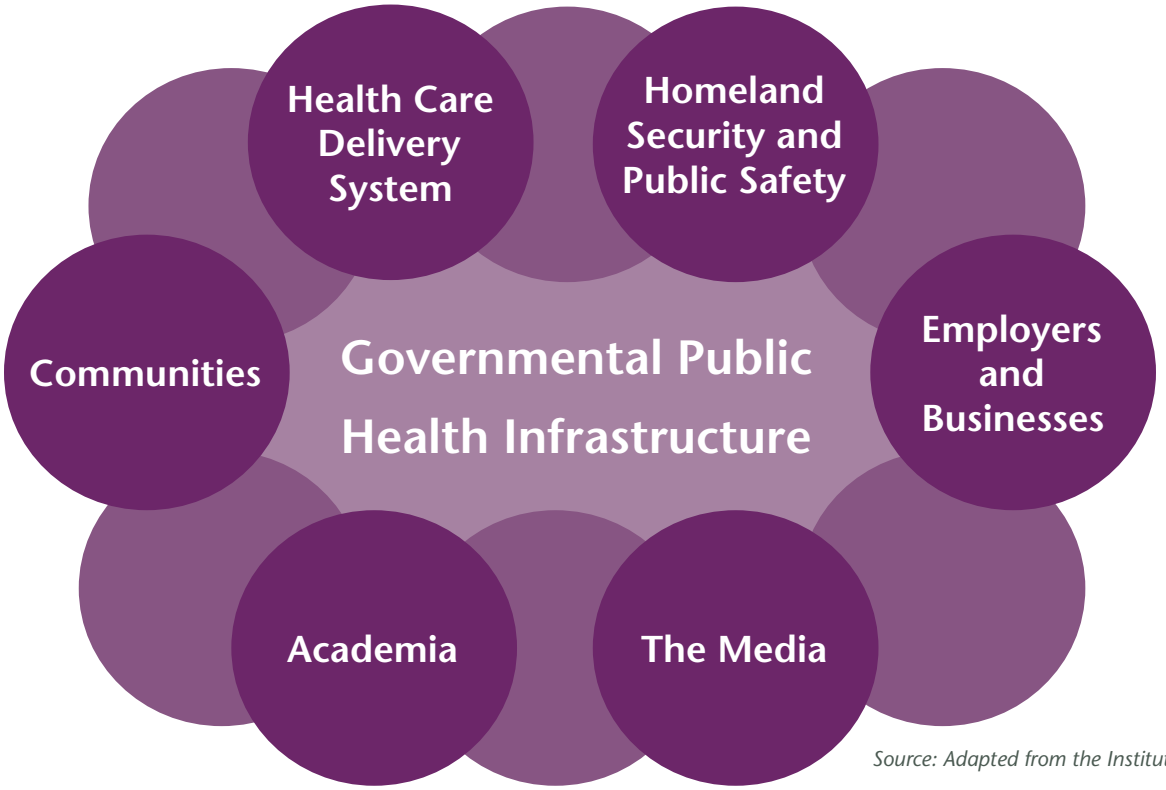
Threats to cyberspace pose a serious economic and national security challenge. A growing array of state and non-state terrorist and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government. Major cyber-attacks to U.S. critical infrastructure systems could result in long-term, wide-scale disruption of services, such as regional power outages. The chance of such attacks is remote because the level of technical expertise and sophistication required, including the ability to create physical damage or overcome mitigation factors like manual overrides, would be out of the reach for all but the most advanced users—such as Russia and China.[24] However, isolated state or non-state groups might deploy less sophisticated cyber-attacks as a form of retaliation or provocation. These less advanced but highly motivated groups could access poorly protected U.S. networks that control core functions, although their ability to leverage that access to cause high-impact, systemic disruptions would probably be limited. However, even unsophisticated attacks could have significant outcomes due to unexpected system configurations or vulnerabilities that could spread throughout a networked system.[25]

Facing the threat of cyber-attacks that could disrupt U.S. power, water, communication, and other critical systems, President Obama in 2013 issued Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience. These policies reinforce the need for holistic thinking about security and risk management. For more information on EO 13636 and PPD 21, visit http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical.

Impact of Cyber-Attacks on Public Health Infrastructure and Health Information Exchange

As people use electronic health data more widely and increasingly rely on networked computer technology to deliver efficient healthcare and public health services, the need to protect public health information and public health infrastructure increases. In 2008, the Institute of Medicine proposed a framework for the Public Health Preparedness System (Figure 1) comprising the following stakeholders:

FIGURE 1. PUBLIC HEALTH EMERGENCY PREPAREDNESS SYSTEM



Source: Adapted from the Institute of Medicine

- Health Care Delivery System;
- Homeland Security and Public Safety;
- Employers and Businesses;
- The Media;
- Academia;
- Communities; and
- Governmental Public Health Infrastructure, an organizational hub for the other stakeholders.[26]

This framework illustrates the interconnected elements essential for public health emergency readiness. While the framework does not explicitly mention information technology, all seven stakeholders heavily use that technology. A cyber-attack on any of the seven stakeholders could result in losses of integrity, availability, and confidentiality or physical destruction in systems that contribute to public health. Table 1 on the following pages shows the effects a cyber-attack could have on each stakeholder in the public health infrastructure.[27]

In addition, a cyber-attack could seriously affect every essential public health service that LHDs perform, as described in Table 2 on page 8. A successful cyber-attack on public health information infrastructure could severely reduce both public health emergency responses and non-emergency public health functions. Further, potential consequences of cyber-attack go far beyond data theft. Cyber-attacks affect physical structures, timeliness of services, and even finances.[28]

Cyber-attacks also threaten the future of health IT interoperability. The Office of the National Coordinator for Health Information Technology surveyed 2,000 individuals to determine how they felt about the electronic use of their health data. About 75% of respondents expressed concern about the privacy and security of their electronic health records. The survey also revealed that almost 10% of individuals had withheld medical information when they learned their providers used electronic health records.[29] Because people often greatly value the privacy of their health data, large-scale data breaches or cyber-attacks may make them less enthusiastic about using electronic health records.

Decreased trust caused by a cyber-attack affects more than just the healthcare sector. The erosion of trust in government communications threatens information-sharing during a disaster. If the information for a community shelter had been damaged or changed during a disaster, individuals might not use the information. This lack of trust in emergency situations poses tremendous risk to public health and safety.

TABLE 1. CYBER THREATS THAT AFFECT PUBLIC HEALTH EMERGENCY CAPACITY

	Losses of Integrity	Losses of Availability	Losses of Confidentiality	Physical Destruction in Systems that Contribute to Public Health
Health Care Delivery System	• Loss of confidence in healthcare providers due to perceptions of inadequate security	• Disruption of care due to software outages: (1) loss of access to health records limits public health's ability to provide appropriate care, shelter, and medicine in times of need; (2) damage to infrastructure such as transit or insurance/payment methods could also prevent people from accessing necessary medical care	• Theft or loss of patient information • Security and privacy risks that emerge in personal medical devices, given their increasingly networked and wireless nature	• Power outages in hospitals caused by the collapse of public power grids • Destruction of generators due to modified code in programmable logic controllers • Security and privacy risks that emerge in personal medical devices, given their increasingly networked and wireless nature
Homeland Security and Public Safety	• Disruption of emergency telephone lines and EMS systems, which could slow or disable emergency medical response	• Disruption of emergency telephone lines and EMS systems, which could slow or disable emergency medical response		• Amplified impact on public health by physical attack of weapons of mass destruction combined with cyber elements
Employers and Businesses	• Reputational damage, financial gain and fraud, commercial advantage, and economic and political damage • Loss of protected health information and subsequent decrease in public trust of health apparatuses	• Inability to produce needed medical equipment or drugs through manufacturing stoppages • Failures of vendors to provide key hospital services ranging from software to temporary staffing	• Reputational damage, financial gain and fraud, commercial advantage, and economic and political damage	• Damage to physical systems used to perform functions, such as regulated utilities, critical to public health that shuts down or slows supply chains, impairs patient care, and impedes emergency response, potentially leading to significant loss of life
The Media	• Corruption or distortion of legitimate information from government or expert sources transmitted via media to the public • Loss of social media during public health response	• Direct or indirect disabling of media transmission/ reception, impairing the ability of public health to reach communities with up-to-date information • Loss of social media during public health response		

TABLE 1, CONTINUED

	Losses of Integrity	Losses of Availability	Losses of Confidentiality	Physical Destruction in Systems that Contribute to Public Health
Academia			• Sensitive academic research that could be used as a weapon or induce a public health crisis	• Power outages affecting laboratories that house infectious agents, cadavers, and research animals
Communities		• Lack of backup generators/systems to maintain vital operations, such as refrigerating food and medication or running medical devices outside of hospitals		• Loss of infrastructure causing the denial of utility services needed to maintain public health • Loss of electricity or water during heat waves or cold spells • Failure of industrial safety systems (e.g., in chemical manufacturing)
Governmental Public Health Infrastructure	• Limited federal, state, and local ability to coordinate public health response and conduct surveillance on the progress of efforts due to impaired availability of command and control infrastructure • Disruption of critical analysis by health informaticians in public health surveillance through threats to data collection, storage, and analysis	• Limited federal, state, and local ability to coordinate public health response and conduct surveillance on the progress of efforts due to impaired availability of command and control infrastructure • Disruption of critical analysis by health informaticians in public health surveillance through threats to data collection, storage, and analysis	• Penetration and improper release of information from initiatives such as CDC's Select Agent Program with respect to dangerous agents and potential countermeasures • Liability for lawsuits against federal, state, and local governments and governmental healthcare organizations due to breaches in record confidentiality	• Unusable components of the public health supply chain and disease surveillance and laboratory systems • Increased strains on a public health system that is already suffering from budget cuts • Reduced ability for workers to access just-in-time training

TABLE 2. IMPACT OF CYBER-ATTACKS ON 10 ESSENTIAL PUBLIC HEALTH SERVICES

Essential Public Health Service	Key Activity Affected	Explanation
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	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
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	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 ensure the provision of healthcare 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.
Ensure competent public and personal healthcare 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.

Recommendations for LHDs

Strategically approaching an organization's cybersecurity efforts can be a big challenge. Some individuals may feel that cybersecurity is too complex to manage properly. However, as mentioned earlier, simple cybersecurity measures can greatly lower the risk of a cyber-attack. As a first step, local health officials can meet with the LHD's chief information officer to determine who is in charge of IT systems and services (IT systems are often managed differently by jurisdiction (i.e., state-run or local-run)). If the LHD does not have a chief information officer, leadership can reach out to the manager of IT systems.

The most basic cybersecurity plan should include the following security practices, at a minimum. The components of this plan are borrowed from the National Institute of Standards and Technology's framework for improving critical infrastructure cybersecurity.[30]

STANDARDIZED POLICIES AND PROCEDURES

LHDs should proactively establish standardized policies and procedures regarding requirements for managing the safety, effectiveness, and security of IT systems, including rules for password protection and data management. The LHD should audit the policies at least once a year and review them with both IT and general staff members to ensure compliance.

PROPER IDENTIFICATION, AUTHENTICATION, AND ACCESS

Identification and authentication techniques such as IDs and passwords enable LHDs to identify system users and confirm that information is from a trusted source. Robust identification and authentication techniques are important to public health because many practitioners collect sensitive data from a variety of sources. LHDs should require that passwords and access codes change frequently to prevent unauthorized users from breaking into systems or shorten the length of time they can access the network.

SECURITY PATCH MANAGEMENT

LHDs should update software packages to fix preexisting bugs or vulnerabilities. Properly managing security patches reduces the risk of a compromised computer system. The LHD's computing policy should require that patches be installed as they become available; software companies often alert users or IT managers when a new patch is available. LHD leaders should understand the IT staff's process for patch management and communicate to all staff the importance of patch management.

SECURITY RISK MANAGEMENT

A cyber-risk assessment is the systematic evaluation of the potential risk that cyber-breach could occur on a network. Risk assessments involve identifying threats, responding to threats, managing threats, and monitoring for new threats. If LHDs provide clinical care and store any kind of electronic health data, they must attest to having completed a risk assessment to OCR. Also, LHDs should consider holding cybersecurity tabletop exercises to prepare for, protect from, and respond to the effects of cyber-attacks. These exercises help to identify policies and issues that hinder or support cyber-attack mitigation response. LHD leaders should speak to IT staff about what process is in place to conduct security risk management.

Conclusion

As the world of public health becomes more digitized, the need to protect the digital information that allows LHDs to save lives is becoming more pressing. As previously mentioned, any LHD, no matter how digitally savvy, can take basic precautions that will help prevent a damaging data theft. Without sound cybersecurity practices, the public's view that its health data are not safe could slow the growth of public health information exchange.

References

1. Friedman, A., & Singer, P.W. (2014) *How it all works. Cybersecurity and Cyberwar: What everyone needs to know* (pp. 12-13). New York: Oxford.
2. Ibid
3. Friedman, A., & Singer, P.W. (2014) *How it all works. Cybersecurity and Cyberwar: What everyone needs to know* (pp. 34-35). New York: Oxford.
4. Office of the Assistant Secretary for Preparedness and Response. (2014). *Healthcare and public health cybersecurity primer: Cybersecurity 101* (HHS Publication). Retrieved October 15, 2014, from http://www.phe.gov/preparedness/planning/cip/documents/cybersecurity-primer.pdf
5. Ibid
6. RedCondor Secure. (2010). *Phishing for disaster: The cost of corporate ignorance.* Retrieved October 15, 2014, from http://www.redcondor.com/resources/whitepapers/0710.phishing-white-paper.pdf
7. Business Insider. (2013) *The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought.* Retrieved November 23, 2014, from http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11
8. DigitalThreat. (2009). *Threat vs vulnerability vs risk.* Retrieved October 19, 2014, from http://www.digitalthreat.net/2009/06/threat-vs-vulnerability-vs-risk/
9. Office of the Assistant Secretary for Preparedness and Response. (2014). *Healthcare and public health cybersecurity primer: Cybersecurity 101* (HHS Publication). Retrieved October 15, 2014, from http://www.phe.gov/preparedness/planning/cip/documents/cybersecurity-primer.pdf
10. Ibid
11. Silicon Flatirons. (2013). *Cybersecurity and cloud computing in the health care and energy sectors: Perception and realities of risk management.* Retrieved October 12, 2014, from http://www.siliconflatirons.com/documents/publications/report/201306cybersecurityreport.pdf
12. Anderson, H. (2012, April 9). Utah health breach affects 780,000. *Data Security Today.* Retrieved August 9, 2014, from http://www.databreachtoday.com/utah-health-breach-affects-780000-a-4667
13. Ibid
14. Reed, T. (2014, Aug. 21). Three reasons why data is such a big target in the health care sector—and what health practices can do about it. *Washington Business Journal.* Retrieved October 8, 2014, from http://www.bizjournals.com/washington/blog/2014/08/3-reasons-why-health-care-data-is-such-a-security.html?page=all.
15. Humer, C., & Finkle, J. (2014, Sept. 24). Your medical record is worth more to hackers than your credit card. *Reuters.* Retrieved October 8, 2014, from http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924?feedType=RSS&feedName=healthNews
16. McCarthy, E. (2014, Aug 18). Community Health Systems says it suffered criminal cyber attack. *Wall Street Journal.* Retrieved October 10, 2014, from http://online.wsj.com/articles/community-health-systems-says-its-suffered-criminal-cyberattack-1408365259
17. Tamburello, L. (2014) As health data proliferates, threats to security grow. *Inside Counsel. Breaking News.* Retrieved November 2, 2014, from ProQuest Central database.
18. American Medical Association. *HIPAA violations and enforcement.* Retrieved November 23, 2014, from http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page
19. Ibid
20. Ibid
21. Department of Health and Human Services. (2010). *Guidance on risk analysis requirements under the HIPAA security rule.* Retrieved October 28, 2014, from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
22. Lucido, S., & Denise, K. (2003). HIPAA privacy rule and public health: Guidance from CDC and the U.S. Department of Health and Human Services. *Morbidity and Mortality Weekly Report.* Retrieved October 28, 2014, from http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

23. Licastro, L. B. (2012). HIPAA/HITECH enforcement action alert. *The National Law Review.* Retrieved January 5, 2015, from http://www.natlawreview.com/article/hipaahitech-enforcement-action-alert

24. Clapper, J. R. (2013). *Statement for the record: Worldwide threat assessment of the US intelligence community.* Senate Select Committee on Intelligence, 1-3. Retrieved December 15, 2014, from http://www.intelligence.senate.gov/130312/clapper.pdf

25. Lyons, M. (2005). *Threat assessment of cyber warfare: A white paper.* Retrieved December 7, 2014, from http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/Lyons-P590TU-White%20paper.pdf

26. Barnett, D. J., Sell, T. K., Lord, R. K., Jenkins, C. J., Terbush, J. W., & Burke, T. A. (2013). Cyber security threats to public health. *World Medical & Health Policy,* 5(1), 37-46.

27. Ibid

28. Ibid

29. McCann, E. (2014). ONC finds consumers distrust EHRs enough to withhold information. *Government HealthIT.* Retrieved November 6, 2014, from http://www.govhealthit.com/news/cms-finds-consumers-distrust-ehrs-enough-withhold-information

30. National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity, version 1.0.* Retrieved January 5, 2014, from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[ISSUE BRIEF]

February 2015

Acknowledgments

This issue brief was made possible through the support of the Centers for Disease Control and Prevention (CDC), cooperative agreement #5U38OT000172-02. NACCHO is grateful for this support. The views expressed within do not necessarily represent the official views of the CDC.

NACCHO would like to acknowledge the following members of NACCHO's ePublic Health and Informatics workgroup for contributing to the creation of this document: Eric Bakota; Chris Collinge; and Joseph Gibson. NACCHO also thanks John Osborn, MS, Operations Administrator, Mayo Clinic; and Stephen Curren, Program Manager, Critical Infrastructure Protection Program, Department of Health and Human Services. NACCHO also acknowledges Justin Snair for his insights and contributions in the fields of critical infrastructure security and emergency preparedness.

FOR MORE INFORMATION, PLEASE CONTACT:

Matthew DeLeon
Program Analyst, Public Health Informatics
202-507-4237
mdeleon@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 be a leader, partner, catalyst, and voice with local health departments.

1100 17th St, NW, 7th Floor Washington, DC 20036

P 202-783-5550 F 202-783-1583

www.naccho.org