July 10, 2020

M E M O R A N D U M

To: Governors' Offices
From: NGA Center for Best Practices: Homeland Security and Public Safety Division
Re: Cybersecurity Concerns for Health and Public Health Organizations

Public health and healthcare organizations are at the forefront fighting against unprecedented physical dangers from the COVID-19 outbreak. Simultaneously, there are threats propagating in cyberspace, as malicious actors target vital public health and healthcare systems. For example, hackers have zeroed in on the U.S. Department of Health and Human Services[1] and the World Health Organization[2] in an attempt to disrupt and undermine these organizations' response to the pandemic. As health organizations rapidly make changes to their infrastructure, cybersecurity resilience should be prioritized, as successful cyberattacks will exacerbate current challenges.

This memo provides the following:

Prevailing Vulnerabilities within Health Information Technology

The healthcare and public health (HPH) sector is a large and diverse sector that provides an array of goods and services that are essential to the health, safety, and well-being of citizens. Critical functions of the sector include, but are not limited to:

- Health plans and payers, who provide payment to caregivers for goods and services related to healthcare;

[1] https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

[2] https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

- A large system of private enterprises that manufacture, distribute and sell drugs, biologics and medical devices;
- Population-based care and surveillance provided by health agencies at the federal, state and local levels; and
- Hospitals and other medical care facilities including the first responders, nurses, doctors and other health professionals that support these facilities.[3]

Public health and healthcare professionals are intrinsically focused on saving lives and providing quality care, not cybersecurity, although it is a priority for patient safety. For example, a healthcare organization in Wyoming fell victim to a ransomware attack that necessitated diverting patients to other hospitals and led to an inability to access patient records to continue care delivery.[4] The organization worked for the next month to get its computer systems back online and consequently had to cancel many exams and procedures.[5]

Cyberattacks such as this can expose sensitive patient information and force already stressed hospital systems to expend scarce resources to recover. Doctors, nurses, and other healthcare professionals understand the importance of hand sanitizing to prevent the spread of germs and should apply this same methodology to improving cybersecurity practices to throughout the organization. Good "cyber hygiene" and a culture of cyber awareness can prevent 80 percent of cyber-attacks.[6] While innovations in health IT can increase optimization and efficiency to address clinical care, fundamental research or population health, the technology will only work if it is secure.

Legacy Information Technology Infrastructure

Utilization of legacy software and systems plagues health and public health organizations, given their useful lifespans, many of these antiquated technologies were not built with cybersecurity in mind. While these systems could still be clinically useful, many may run insecure software and hardware, which leaves them vulnerable to attacks. For example, recent research suggests that an estimated 83 percent[7] of medical imaging devices used throughout U.S. healthcare systems are currently running on outdated operating systems.[8] However, for some hospitals and public health organizations, it is not financially feasible to replace these technologies even with the increased concern among health professionals for cyberattacks.[9,10]

Medical Record Systems and Medical Devices Security

---

[3] https://www.phe.gov/Preparedness/planning/cip/Documents/cybersecurity-primer.pdf

[4] https://county17.com/2019/09/20/disaster-declared-in-wake-of-hospital-ransomware-attack/

[5] https://www.cchwyo.org/News/Press_Center/Health_News/2019/Service_Disruptions_at_CCH_no_ETA.aspx

[6] European Union Agency for Network and Information Security (ENISA). December 2016. Review of Cyber Hygiene Practices. https://www.enisa.europa.eu/publications/cyber-hygiene/

[7] https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[8] https://support.microsoft.com/en-us/help/4057281/windows-7-support-ended-on-january-14-2020

[9] The American Medical Association in conjunction with Accenture surveyed 1,300 physicians in the United States to assess their experience and attitudes toward cybersecurity.

[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/

Healthcare organizations have long been an attractive and lucrative industry for threat actors because personal health information (PHI) is more valuable on the black market than many other types of personally identifiable information (PII).[11] This information is exchanged throughout the public health system which is comprised of all public, private, and voluntary entities that contribute to the delivery of essential public health services within a jurisdiction. Therefore, cyber criminals have a higher incentive to target medical databases for personal gain. According to the U.S. Department of Health and Human Services, more than 15 million health records have been compromised due to data breaches.[12] A public health system where information and data is exchanged securely and promptly with clinicians improves the coordination of care throughout each functional level. If the real-time flow of information and data is blocked – due to interoperability challenges or a security breach – then effective therapeutic interventions cannot be delivered. With the proliferation of electronic health record technologies within the critical functions of the HPH sector, it is vital for key stakeholders to address and manage the risks associated with cyber threats to HPH systems.

For example, due to the COVID-19 crisis, hospitals are using patient monitoring devices, such as vital-sign sensors, more than ever.[13] These patient monitoring devices can be used remotely and deliver critical information to medical professionals to adequately treat a patient's needs. Enabling devices to have remote access, however, increases the attack surface due to its increasingly networked and wireless nature. Medical device manufacturers are required by the U.S. Food and Drug Administration to comply with security regulations that include monitoring, identifying, and addressing cybersecurity vulnerabilities in medical devices once they are on the market.[14]

Cybersecurity threats and vulnerabilities can impact the confidentiality, availability, and integrity of IT networks and the medical devices connected to these networks. A distributed denial-of-service (DDoS) attack could potentially have devastating physical consequences for patient care if systems are compromised and contribute to a loss of confidence in healthcare providers.[15,16]

Preparedness and Readiness Challenges

Within the healthcare industry, professionals are focused on providing quality patient care. They understand how to use technologies to make more accurate diagnoses and provide better treatment to patients but may not easily understand the risks surrounding cybersecurity. Many health organizations have limited funding for cybersecurity resources, limited education and awareness programs for healthcare professionals, and lack dedicated cybersecurity personnel.[17] With the magnitude of the threat growing exponentially, the funding

---

[11] https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/

[12] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[13] https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-allows-expanded-use-devices-monitor-patients-vital-signs-remotely

[14] https://www.fda.gov/media/123052/download

[15] A distributed denial-of-service attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more servers.

[16] Choo, Kim-Kwang Raymond. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. Computers & Security. 30. 719-731. 10.1016/j.cose.2011.08.004.

[17] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/

required to secure this information has lagged in comparison to other industries.[18] The primary focus for any HPH organization is care, but stakeholders also must shore up their defenses to protect their digital infrastructure.

Lack of investment is not only a challenge in the private sector. Members of public health departments also report that without experiencing a security breach or data loss, many have difficulty demonstrating the importance of cyber protections and how proactive risk mitigation can save money and protect against damage long-term.[19] In a survey conducted by the National Association of County and City Health Officials (NACCHO), local health departments (LHDs) ranked cybersecurity as one of their top three concerns. Yet, when it comes to specific preparedness actions, like running a cyberattack exercise, LHDs most often report that they have not conducted preparedness activities in this topic area.[20] In a survey delivered to emergency managers within a statewide hospital association found that only a third of respondents had an all-hazards plan and a continuity of operations plan that could be used during a cyberattack.[21] Making the decision to prioritize and resource cybersecurity in public health will require organizational culture shifts, increased financial resources, the appropriate personnel and support from leadership to create a robust cyber preparedness plan. Agencies must also consider applicable federal and state legal requirements for ensuring the security of electronic health records, such as the HIPAA Security Rule."

Current Threat Landscape for Healthcare and Public Health Organizations

With healthcare resources being stretched due to the COVID-19 response, cybercriminals have increased the number of attacks targeting hospitals and government public health organizations.[22]

Cyber espionage: Russian, Chinese, North Korean and Iranian hacking organizations have used COVID-19 as a lure in their campaigns.[23] A cybersecurity firm reported that a Chinese hacking group, Advanced Persistent Threat 41 (APT41),[24] carried out a broad hacking campaign during the onset of the pandemic.[25] APT41 is a sophisticated Chinese state-sponsored group that specializes in espionage against healthcare, high-tech, and

---

[18] https://techcrunch.com/2018/08/09/the-healthcare-industry-is-in-a-world-of-cybersecurity-hurt/

[19] https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

[20] https://www.naccho.org/uploads/downloadable-resources/2018-Preparedness-Profile-Report_external_final.pdf

[21] https://researchrepository.wvu.edu/cgi/viewcontent.cgi?article=4749&context=etd

[22] https://cyber.nj.gov/alerts-advisories/cyber-threats-cybersecurity-for-healthcare-during-covid-19. For more on the current threat landscape and additional recommendations to address these issues, see NGA's Cybersecurity and COVID-19 Memorandum, which details recommendations for state governments looking to collaboratively encourage cyber resilience for private sector healthcare partners. https://www.nga.org/wp-content/uploads/2020/04/COVID-Cybersecurity-Memo.pdf.

[23] https://www.us-cert.gov/ncas/alerts/AA20126A

[24] Advanced Persistent Threat (APT) is an attack in which an unauthorized user gains access to a system or network and remains there for an extended period of time without being detected.

[25] https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

political interests.[26] This campaign sought to exploit vulnerabilities in networking equipment, cloud software, and telehealth services during this pandemic.

Social Engineering: Hackers use social engineering to manipulate the natural human tendency to trust and gain access to sensitive information. The FBI issued a warning to alert the general public that nefarious culprits are quickly adapting their social engineering tactics, techniques, and procedures to take advantage of the current public health emergency.[27] Credential phishing campaigns have directly targeted U.S. healthcare organizations with emails that claim to provide COVID-19 financial relief to adults.[28]

Ransomware: There has been a significant increase in the number of attempted ransomware attacks against health and public health organizations.[29] Cybercriminals are using ransomware to hold hospitals and medical services hostage unless a ransom is paid. As most organizations have moved to a remote workforce, hackers have identified a new target: virtual private networks (VPN).[30] Once a network is infiltrated, adversaries can perform thorough reconnaissance, gaining privilege and access to systems based on security weaknesses.[31]

Actors are also employing social engineering related spoofing,[32] smishing,[33] and vishing techniques to give off the impression of authenticity, which leverages the misplaced trust in the security of phone services.

Cybersecurity Best Practices for Health and Public Health Organizations[34]

Define and Streamline Cyber Governance: Cybersecurity is an elected official or C-suite level issue, as senior leaders are owners of any associated risk due to the negative impacts cyberattacks may have on the entity overall. As the chief executive of their state, for example, governors have a strong leadership role to play in mitigating cyber risk. Cyber resilience can only be achieved with active engagement from the top. While assuming the responsibility as risk owner, senior leadership should delegate cyber risk management experts to drive an enterprise wide cybersecurity strategy. The cybersecurity leader helps to define roles and responsibilities and coordinates with relevant stakeholders to adopt a cybersecurity framework. Any good governance model should actively include non-traditional personnel outside of IT professionals and device manufacturers (i.e., Administrators, HR personnel, Finance and the Emergency Management departments).

---

[26] https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html

[27] https://www.ic3.gov/media/2020/200320.aspx

[28] https://www.us-cert.gov/ncas/alerts/aa20-099a

[29] https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

[30] https://www.us-cert.gov/ncas/alerts/aa20-107a

[31] https://www.microsoft.com/security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-what-to-do/

[32] Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.

[33] Smishing is any kind of phishing that involves a text message.

[34] *Healthcare Industry Cybersecurity Taskforce: Report on Improving Cybersecurity in the Healthcare Industry*, https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

This holistic approach ensures cybersecurity is effectively communicated to leadership to gain stakeholder buy-in to increase resources availability.[35]

Upgrade or Secure Legacy Systems: Health and public health organizations must: (1) take inventory of their clinical environments and document unsupported operating systems, devices and electronic health record systems; (2) replace or upgrade legacy or unsupported systems where possible; (3) leverage network segmentation and other risk reduction tools to increase the security and resilience of medical devices and health information technology.

Employ Identity and Access Management Tools: Defining the roles and access privileges of users and the circumstances in which users are granted or denied those privileges is the cornerstone of any secure network. By ensuring that employees only have access to data that is essential to their jobs, organizations can significantly limit the scope of their potential attack surface. Tools like **multifactor authentication –** two-factor authentication, especially for remote access, ensures that a compromised password cannot alone be used to gain access – provide greater assurance.

Improved Cybersecurity Awareness and Education: HPH organizations must effectively convey to employees the heightened risk of social engineering attacks tied to COVID-19 that exists at the present time. In addition, employers must also provide their workers with the knowledge and tools they need to effectively handle and defuse any attempted social engineering attacks they may encounter. In particular, organizations should properly educate their workforces on how to spot and address social engineering scams in real time. Beyond training employees on how to identify these attacks, employers should provide their workers with guidance on proper cybersecurity practices to follow.

Improve information sharing of industry threats, risks, and mitigations. Information should be tailored in a way that makes for easier consumption by small and medium-size organizations that rely on limited or part-time security staff. Organizations should consider joining the Health Information Sharing and Analysis Center (H-ISAC)[36] to have a broad scope and further reach when it comes to information sharing across the healthcare industry. Organizations should focus on creating more effective mechanisms for disseminating and utilizing data from the H-ISAC.

Response Planning: It is imperative for healthcare and public health organizations to implement and maintain incident response and disaster recovery plans that can be activated immediately with adequate resources to respond to an executed cybersecurity attack mentioned above. Organizations should also review their plans with key personnel to ensure that everyone is up-to-speed on their roles and responsibilities in the event the plan needs to be put into action. Exercising incident response plans helps all relevant stakeholders to deconflict contingencies and quickly address lesson learned to improve such plan.

[35] Resources include funding, personnel and training and awareness programs.

[36] https://h-isac.org/

Conclusion

Cyber criminals are continually adjusting their tactics to take advantage of new situations and the current COVID-19 public health crisis is no exception. Malicious actors are working feverishly to take advantage of the public's concern over the health crisis and its high appetite for COVID-19-related information, which presents a prime opportunity to utilize social engineering methods to deliver malware and ransomware, therefore stealing user credentials. As the world continues to grapple with the COVID-19 pandemic, public health and healthcare organizations must sufficiently invest in resources to mitigate risk and reduce vulnerabilities resulting from software, hardware, and humans relying on both to deliver critical services.

For questions or concerns related to the contents of this memo, please contact NGA staff:

- *Khristal Thomas (kthomas@nga.org; 202.624.7810)*
- *Maggie Brunner (mbrunner@nga.org; 202.624.5364)*

Funding for this memo was made possible (in part) by the Centers for Disease Control and Prevention. The views expressed do not necessarily reflect the official policies of the Department of Health and Human Services.