ASPR TRACIE Technical Assistance Request

Request Receipt Date (by ASPR TRACIE): 17 February 2022
Response Date: 14 March 2022

Request:

The requestor asked for information on high-profile healthcare cyberattacks over the past five years in the U.S., to include resources and details on the associated impacts and lessons learned for clinical care delivery.

ASPR TRACIE Resources

Cybersecurity Resource Page

Cybersecurity Topic Collection

Healthcare System Cybersecurity Readiness and Response Considerations

Healthcare System Cybersecurity: Readiness & Response Considerations Speaker Series Presentation

Response:

A preliminary review of cyberattacks in the healthcare industry over the past five years shows that **cyber-related crime on healthcare systems continue to increase at an alarming rate**. Since the 2017 U.K. "*WannaCry*" cyber incident, there have been, on average, 300+ attacks per year on healthcare organizations.

ASPR TRACIE subject matter experts (SMEs), many of whom have had firsthand experience with cyber challenges in their healthcare systems, note that **most healthcare systems face "phishing," denial of service, and other types of attacks on a routine basis**. Malware attacks that infiltrate clinical systems, paralyze operations, or reveal protected health information are common and require aggressive defensive measures and preparedness. Moreover, **many cyberattacks do not target healthcare institutions directly, but instead infiltrate third-party vendors resulting in devastating unintended consequences to U.S healthcare systems**. "NotPetya" is a prime example of this type of attack, where healthcare facilities were not the intended target, but because healthcare-related vendors were infiltrated, significant impacts disrupted healthcare delivery capabilities.

Section I of this document lists the major impacts to healthcare services as a result of cyberattacks, ***Section II*** includes considerations for healthcare emergency planners to incorporate in their planning efforts, and ***Section III*** lists notable recent healthcare-related cyber incidents. More in-depth information on these incidents can be found in the HHS Health Sector Cybersecurity Coordination Center (HC3) main page and ***Section IV***'s related resources.

ASPR TRACIE thanks the following SMEs for their contribution to this response: ***Melissa Cole Harvey*** *RN, BSN, MSPH, Assistant Vice President, Enterprise Preparedness & Emergency Operations HCA Healthcare****; Craig DeAtley****, PA-C, Director, Institute for Public Health Emergency Readiness, MedStar Washington Hospital Center;* ***John Hick,*** *MD, Hennepin Healthcare, ASPR TRACIE Senior Editor;* ***Shelly Schwedhelm****, MSN, RN, NEA-BC Executive Director, Emergency Management and Biopreparedness, Nebraska Medicine and Global Center for Health Security.*

I. Major Impacts to Healthcare Services

The following are examples of critical operational healthcare components that may be impacted during a Cyberattack on healthcare entities, including significant affects on their services:

- Electronic hospital communications (paging, phone, alerting systems)
- Internet services
- Utilities (via attacks on utilities providers)
- Lab, radiology, PACS, pharmaceutical orders/results
- Supply chain management
- Electronic health records (EHR), patient data/history
- Connected biomedical devices
- Patient-facing applications and portals
- Patient therapies
- Financial systems (expensive recovery costs, technical remediation needs)
- Onsite security/patient safety (lock/access controls, badging, etc.)
- Health insurance/Medicaid/Medicare billing and data compromise
- Credentials, licensing
- Diverted payroll
- Delayed care, limited/cancelled medical procedures
- Web-based clinical resources, research databases, disease registries
- Food/nutrition services
- Patient, community trust

II. Healthcare Cybersecurity Considerations

The following information is a summarized compilation of lessons learned related to recent cybersecurity incidents. The ASPR TRACIE Team identified several major themes across the reports, articles, and documents reviewed. The following is a snapshot/summary of the findings, and not an exhaustive list of all lessons learned.

Major Categories of Lessons Learned:

1. *Preparing the People*: Employee Awareness and Cyber Hygiene
2. *Preparing the Organization*: Policies and Procedures
3. *Understanding Vulnerabilities*: Risk Assessments, Continuous Monitoring
4. *Having a Response Strategy*: Training/Preparedness, Communication/Information Sharing
5. *Hardening Cyber Infrastructures*: Access Controls, Redundancy, Patching, Encryption

General Assumptions and Promising Practices:

- **Know your facilities' major risks, vulnerabilities, and dependencies**. Healthcare facilities should think of a potential attack as a "when" not "if" scenario. Prioritize critical data and cyber assets. Determine what type of attack those assets are most vulnerable to. If systems go down, think through what elements of information will be missing/restricted/limited, what workflows will be impacted, and what type of backups can be prepared ahead of time (e.g., medical orders, options for new workflows).

- **Have the right team and experts in place to assess organizational technologies, map systems and networks**. Verify appropriate system defenses are in place (e.g., labeling external emails, implementing "phishing" education, firewalls). Ensure regular vulnerability assessments are conducted. Are technical teams keeping software patches up to date? Are proper patching protocols implemented? If technical experts are not available to assist with risk assessments, identify where to find free support services via regional/federal cybersecurity agencies. Many offer no-cost resources and support.
- **Exercises and training are critical.** Continuously train/test staff on recognizing a cyberattack attempt and reporting an incident. Use multiple scenarios for preparedness exercises and training. Plan for multiple systems being down at one time and practice a mix of issues/limitations. Plan for concurrent disasters (e.g., a cyber incident amid a public health emergency/patient surge). Consider using planned outages to train staff and incident command managers. Engage local law enforcement, risk managers, third-party vendors, insurers, and ancillary services in exercise and training efforts.
- **Ensure all necessary downtime procedures are in place**. Expect to use them for extended periods of time. From the list in Section I consider what capabilities may be impacted and what replacement processes and supplies may be needed (e.g., pen/paper orders, charting, billing). Consider use of downtime safety officers/coaches and just-in-time training. Have proper supplies on-hand with a plan for distribution.
- **Ensure copies of staffing/patient schedules, critical contact information, stakeholder/vendor data, and contracts/agreements are available offline**. Coordination with partners, stakeholders, regional and federal cybercrime partners is key. Have plans in place to share information and engage external partners. Become familiar with third-party vendor/contractor downtime procedures, support capabilities.
- **Update/integrate/regularly test cyber incident response/business continuity plans** as a hallmark strategy for disaster mitigation. Use real-world cyber events as examples of a healthcare vulnerability to prompt frequent review of business continuity plans; include unique nuances of your organization that should be considered. Engage local law enforcement, hospital risk management, and insurance company(s) in plan reviews. Ensure leadership understands their role in recognizing threats and the thresholds for implementing a cyber response plan. Know who has the authority to shut down a system and/or network. Who is the backup? What if an incident occurs during a holiday or after hours? Are there business continuity plans in place for all critical facility operations?
- **Understand the vulnerabilities that exist in devices, technologies, tools, software, and third-party technology that are deployed across the facility/enterprise**. Cyber readiness is not only about securing a healthcare organization's systems. It is also critical to know what vulnerabilities a vendor may have. Focus should be place on connected medical devices/equipment and any new technologies such as telehealth applications and collaboration tools and platforms. Secure and continuously assess administrative privileges and authentication protocols. Know what redundancy measures are in place including backup and access vulnerabilities.
- **Establish a "cybersecurity culture" within your facility/organization**. Ensure cyber hygiene practices are well established, updated, and communicated across the organization. Expect human error to play a part in cyber vulnerabilities, and ensure staff understand how to protect critical systems and recognize the differences among cyber

scams and attack strategies. Provide real-world examples to keep informed of the latest incidents, threats, and alerts.
- **Establish information sharing processes and protocol for the response phase**. Proper messaging to patients and staff is key. Know what type of information should (and can) be shared to protect the healthcare brand while mitigating risk and taking law enforcement recommendations into consideration.

III. Notable Recent Healthcare-Related Cyber Incidents

The following examples illustrate noteworthy, widely publicized cyberattacks from the past five years that affected healthcare operations and clinical care delivery. It is important to note that this is not an exhaustive list; the number and severity of incidents continues to grow. These examples were chosen based on size, duration, and severity (e.g., over 200,000 patients or records affected). ASPR TRACIE recommends subscribing to the Cybersecurity and Infrastructure Security Agency (CISA) National Cyber Awareness System Alerts for the most current information.

- WannaCry (2017): 4 years (reported to be ongoing), 150 countries affected, 40% of healthcare industry impacted, billions in damages
- NotPetya (2017): Heritage Valley Health System, Princeton Community Hospital, Merck among impacted; over $10B in fiscal damages
- Airway Oxygen (2017): home medical supplier, 500,000 patients impacted
- Bronx-Lebanon Hospital Center (2017): upwards of millions of patients affected
- LifeBridge Health (2018): 500,000 patients compromised
- LabCorp Diagnostics (2018): millions of patient records compromised
- UnityPoint Health (2018): 1.4 million impacted- phishing attack
- University of Virginia Health System (2018): 19 months long- malware attack
- GE Anesthesia Machines (2019): allowed modifications to anesthetic agent composition
- Universal Health Services (2020): $67million in losses, 400 facilities impacted
- University of Vermont Health Network (2020): Month-long EHR downtime, National Guard deployed
- Blackbaud (2020): Trinity Health, INOVA Health Systems, and Rady Children's Hospital among affected; over 4 million patient records affected
- Accellion Software (2021): Trinity Health, University of Miami Health, and Centene among health systems impacted; over 2 million records compromised

IV. Related Healthcare Cyber Attack Resources

The ASPR TRACIE team focused on major cyber-related healthcare disasters that occurred in the U.S. over the last 5 years, mainly referencing industry articles and reviews; a list of official federal and regional cybersecurity guidance can be found in the reference box above. The following is a list of resources outlining major lessons learned and impacts to healthcare.

Abraham, C., Chatterjee, D., Sims, R.R. (2019). Muddling Through Cybersecurity: Insights from the U.S. Healthcare Industry. Business Horizons. 6294): 539-548. (Abstract Only).

American Hospital Association. (n.d.). Ransomware Attack Victims Speak Out: Best Practices & Lessons Learned from Ransomware Attacks. American Hospital Association. (Accessed 3/10/2022).

Argaw, S.T., Bempong, N.E., Eshay-Chauvin, B., et al. (2019). The State of Research on Cyberattacks Against Hospitals and Available Best Practice Recommendations: A Scoping Review. BMC Medical Informatics and Decision Making. 19(10).

Breece, S. (2021). The Non-Negotiable for Health Organizations: Cybersecurity Protection. Cerner Intelligence Blog.

Coden, M., Czumak, M. (2021). How Health Care Providers Can Thwart Cyber Attacks. Boston Consulting Group.

Cyberpeace Institute. (2021). Cyberattacks on Healthcare.

Davis, J. (2017). 10 Biggest Weaknesses and Lessons Learned from Cybersecurity in 2016. Healthcare IT News.

Davis, J. (2018). Biggest Challenges, Lessons Learned from Health Cybersecurity in 2018. Health IT Security.

Garrett, R. (2019). Lessons Learned from a Targeted Ransomware Attack. Modern Healthcare.

Gibbons, S., Nigrin, D., Wood, L. (2018). Surviving a Cyber Attack: An Operational Perspective. Boston Children's Hospital, Healthcare Information and Management Systems Society.

Guy, M., Ghafur, S., Kinross, J., et al. (2018). WannaCry- A Year On. British Medical Journal. 361: K2381.

Health and Human Services (HHS) Cybersecurity Program, Office of Information Security. (2021). 2020: A Retrospective Look at Healthcare Cybersecurity.

Health IT Security. (2021). Scripps CEO Reveals Lessons Learned from Ransomware Attack. (Accessed 3/10/2022).

Jalali, M.S., Russell, B., Razak., et al. (2018). EARS to Cyber Incidents in Health Care. Journal of the American Medical Informatics Association. 26(1): 81-90.

Jefferson, B. (2021). 5 Cybersecurity Lessons Learned from COVID-19. Lepide Data Security and Compliance Blog.

Kessler, D. (2020). Five Cyber-Security Lessons Learned from the Pandemic. Compliance Week.

Kuttler, H. ((2020). You've Been Hacked! Lessons Learned from a Cyber Breach. American Academy of Physician Associates (AAP).

Landi, H. (2020). Healthcare Data Breaches Hit All-Time High in 2021, Impacting 45M People. Fierce Healthcare.

Latham and Watkins Information Law, Data Privacy and Cybersecurity and Healthcare and Life Sciences Practices. (2017). How Can Healthcare Organizations Prepare for the Next Cyberattack? (Accessed 3/10/2022).

McGee, M.K. (2020). Universal Health Services Network Outage: Lessons to Learn. Bank Info Security.

Meuse, B. (2021). Helping Healthcare Win Its Other Big Battle: Cyberattacks. CSO Media, IDG Communications.

Osterman Research. (2020). Cyber Security in Healthcare.

Parker, Smith and Feek. (2020). Lessons Learned from 2020 Healthcare Breaches. (Accessed 3/10/2022).

Raths, D. (2018). Six Lessons Learned from the Boston Children's 'Hacktivist' Attack. Healthcare Innovation Cybersecurity.

Sundaresan, B. (2020). Cybersecurity Lessons Learned from Data Breaches and Brand Trust Matters. Help Net Security.

Symantec. (2018). Cyber Security and Healthcare: An Evolving Understanding of Risk.

U.S Cyberspace Solarium Commission. (2020). Cybersecurity Lessons from the Pandemic.

Weinick, E.B. (2022). Hospitals Run the Cybersecurity Gauntlet. Security Infowatch Healthcare.

Wise, S. (2020). Lessons Learned from the Universal Health Services Cyber Attack. Medical Economics.