ASPR TRACIE Technical Assistance Request

Request Receipt Date (by ASPR TRACIE): 17 February 2022
Response Date: 14 March 2022
Updated: October 3, 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
- The Exchange: Issue 2

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), with firsthand experience managing cyber challenges, note that **most health systems face cyberattacks on a routine basis, with the most common being, phishing, ransomware, data breach, and denial of service attacks**. Many, such as malware, infiltrate clinical systems, paralyze operations, and reveal protected health information, requiring aggressive defensive measures. **Often, cyberattacks do not target healthcare institutions directly, but instead exploit third-party vendor vulnerabilities that result in devastating unintended consequences**. "NotPetya" is a prime example where an attack on healthcare-related vendors led to significant disruptions on healthcare delivery capabilities.

Section I of this document lists major impacts to healthcare services that result from a cyberattack, ***Section II*** includes considerations for healthcare emergency planners, ***Section III*** lists notable recent healthcare-related cyber incidents, and ***Section IV*** provides information on cyber vulnerabilities and reporting requirements. ***Section V*** lists all 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 effects on services:

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

II. Key Considerations for Healthcare Cybersecurity

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 that were reviewed. The following is a snapshot of the findings, and not an exhaustive list of all lessons learned.

Major Categories of Lessons Learned:

1. *Prepare the People*: Employee Awareness and Cyber Hygiene
2. *Prepare the Organization*: Policies and Procedures
3. *Understand Vulnerabilities*: Risk Assessments, Continuous Monitoring
4. *Have a Response Strategy*: Training/Preparedness Planning, Information Sharing
5. *Harden the Cyber Infrastructures*: Access Controls, Redundancy, Patching, Firewalls

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 of cyber experts in place** to assess and map organizational technologies, systems, and networks. Verify appropriate system defenses are in place (e.g., external email labels, firewalls, access controls). Ensure regular vulnerability assessments are conducted. Are technical teams keeping software patches up to date? Are proper protocols in place? If technical experts or resources are not available to assist with risk assessments, know where to find free support services. Many regional/federal cybersecurity agencies offer no-cost resources (see Section IV).
- **Know what cyber-related insurance policies, coverage, and legal resources are in place.** Determine what legal services may be available during or after a cyberattack. Understand the coverage offered, including liabilities and benefit limits, and verify the coverage is sufficient for your facility and/or health system. Plan for how legal or regulatory requirements, or penalties may impact clinical care capabilities or operations.
- **Implement continuous cyber threat education and training.** Ensure staff are up to date on critical security awareness training and safe computing guidelines. Test them on recognizing a cyberattack attempt and ensure they understand how/when/what to report. Use multiple scenarios in preparedness exercises; train for a combination of system failures, downtime issues, and operational limitations; plan for concurrent disasters (e.g., a cyber incident amid a public health emergency/patient surge). Use planned outages to reinforce training. Engage local law enforcement, local emergency managers, third-party vendors, insurers, and ancillary services in planning and response exercises.
- **Ensure specific cyber-related downtime procedures are in place**. Plan to use them for extended periods of time. From the list in Section I consider what operational and clinical care capabilities may be impacted. Identify what replacement processes and supplies may be needed (e.g., pen/paper for orders, charting, billing). Consider establishing downtime safety officers or coaches and just-in-time training. Have proper supplies on-hand with a plan for distribution and updating procedures as needed.
- **Ensure copies of key information are available offline.** Include staffing/patient schedules, stakeholder/vendor contact information, contracts/agreements, software/ application data. Become familiar with third-party vendor/contractor downtime procedures, support capabilities. Plan for how to access critical diagnostic or clinical data. What if software, records, documents, repositories, databases are compromised?
- **Update/regularly test cyber incident response and business continuity plans**. Use real-world cyber events to prompt frequent review of business continuity and incident response plans. Include nuances of your organization that should be considered and engage local law enforcement, hospital risk management, and insurance company(s) in plan reviews. Ensure leadership understands their role in recognizing threats and thresholds for implementing a cyber response plan. Know who has authority to shut down a system/network. Who is backup? What if an incident occurs during a holiday, after hours? Are continuity plans in place for all critical facility operations?
- **Know what vulnerabilities exist in third-party technologies** including, medical devices, tools, and software, that are deployed across the facility/enterprise. Cyber resilience is about securing a healthcare organization's systems, but also knowing what vulnerabilities exist for vendors. Focus on connected medical devices/equipment and 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**. Work towards expanding cyberthreat awareness across the organization. Ensure cyber hygiene practices are well established, updated, and consistently communicated. Expect human error to play a part in cyber vulnerabilities. Ensure staff understand how to protect critical systems, recognize cyber scams, and attack strategies. Maintain situational awareness, know where to find up-to-date information on cyber incidents and threats. Have processes in place to receive and communicate critical alerts; keep staff, critical partners, and external vendors informed of relevant threats specific to your organization.
- **Establish efficient communication, reporting, and information sharing processes.** Have information sharing policies/communication plans in place to ensure proper messaging to patients, staff, and external partners. Know what information should (and can) be shared to protect the healthcare brand while mitigating risk. Establish internal alerting protocol (for staff) and external reporting processes (for partners/stakeholders). Know how and when to involve regional and federal cybercrime partners (e.g., CISA, FBI) and other representatives (legal, insurance). Confirm how vendors will communicate their cyber incidents to your healthcare organization (who to call, where to send) to ensure information is effectively communicated to proper authorities.

III. Notable Cyber Incidents in Healthcare

The following examples illustrate noteworthy, or widely publicized, cyberattacks from the past five years that affected healthcare operations and clinical care delivery. It is important to note this is not an exhaustive list and the number and severity of incidents continues to grow. These examples were chosen based on size, duration, and severity (e.g., over 500,000 patients or records affected). ASPR TRACIE recommends subscribing to the following federal sites for the most current information on these and other incidents: CISA National Cyber Awareness System Alerts; HHS Health Sector Cybersecurity Coordination Center (HC3) main page

- WannaCry (2017): Reportedly 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
- Universal Health Services (2020): $67million in losses, 400 facilities impacted
- University of Vermont Health Network (2020): EHR down, National Guard deployed
- Blackbaud (2020): INOVA Health Systems, Rady Children's Hospital among dozens affected; over 10 million patient records affected
- Accellion Software (2021): Trinity Health, University of Miami Health, and Centene among health systems impacted; over 2 million records compromised
- Scripps Health (2021): Ransomware losses exceed $113million over 4-week period
- Shields Health Care Group (2022): Data breach affects 2 million patients, 60 facilities
- Yuma Regional Medical Center (2022): Ransomware attack impacts 700,000 patients
- Partnership Health Plan (2022): Victim of Hive cybercriminal group affects over 850,000

IV. Cybersecurity Vulnerabilities and Reporting

To maintain heightened situational awareness of new and ongoing cyberthreats and cybercriminal targets, the ASPR TRACIE team encourages healthcare facilities to sign-up for and regularly review the information and alerts available on the following federal sites:

- HHS Healthcare and Public Health Sector: Highlights- Cybersecurity Edition
- HHS 405(d)- Subscribe to The Post
- CISA: National Cyber Awareness System Bulletins/Reports; Sign-up for Alerts
- CISA: SHIELDS UP webpage
- CISA: Stop Ransomware webpage

For additional cyber incident information, the U.S Department of Health and Humans Services maintains an online Breach Portal listing current cases of unsecured health information under investigation. It includes links to specific cases and guidance on filing a report.

To further reduce cybersecurity risks, CISA has also compiled a list of free cybersecurity tools and services healthcare organizations can use to identify cyber vulnerabilities. And, the CISA Known Exploited Vulnerabilities (KEV) catalog and Bad Practices webpage provides detailed information on cyber threats and behaviors that can endanger a facility or organization.

As threats against healthcare systems grow, Federal cyber entities urge rapid reporting of all cyber incidents as they are identified, and to keep reporting threshold levels low. In March 2022, minimum reporting requirements were introduced via the passing of the Strengthening American Cybersecurity Act. If/when fully passed, it would require critical infrastructure organizations, such as healthcare entities, to report any substantial cyber incidents to CISA within 72 hours, regardless if a breach was successful.

- To comply with any new reporting requirements, health systems should ensure future cyber incident response plans incorporate federal reporting mandates into their policies.
- Currently, SMEs urge organizations to contact proper authorities immediately if they believe they have been impacted. Reporting can include any small or unusual incident (e.g., reboots, abnormal system behavior).
- Rapid reporting to CISA and/or the FBI can enable the rapid provision of support/ response services for impacted organizations.

To report anomalous cyber activity and/or cyber incidents to CISA, email report@cisa.gov or call (888) 282-0870. You may also report ransomware incidents via the CISA Incident Reporting System and/or through the FBI Internet Crime Complaint Center (IC3).

V. Related Healthcare Cybersecurity 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 10/3/2022).

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).

Association of Healthcare Emergency Preparedness Professionals. (2020). Cybersecurity in Healthcare. AHEPP Webinar Recordings.

Cimpanu, C. (2019). Vulnerabilities Found in GE Anesthesia Machines. ZDNet.

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. (2017). 500,000 Affected in Ransomware Attack on Home Medical Equipment Supplier. Health IT News.

Davis, J. (2018). 1.4 Million Patient Records Breached in UnityPoint Health Phishing Attack. Healthcare IT News.

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

Davis, J. (2018). LabCorp Goes Down After Network Breach, Putting Millions of Patient Records at Risk. Healthcare IT News.

Davis, J. (2018). Malware Attack on UVA Health Gave Hacker Access for 19 Months. Healthcare IT News.

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

HIPPA Journal. (2022). Healthcare Cybersecurity.

Ipro Tech. (2022). Healthcare Organizations Continue to Be Under (Cyber) Attack.

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. (2022). Healthcare Data Breach Costs Reach Record High at $10m Per Attack: IBM Report. Fierce Healthcare.

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

Lehmann, C. (2022). Don't Wait for a Cyberattack; Know What Coverage You Have Now. Medscape Medical News.

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

McKeon, J. (2022). Exploring Challenges, Benefits of Cyber Insurance in Healthcare. Health IT Security.

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

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

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

Sanborn, B.J. (2018). LifeBridge Health Reveals Breach that Compromised Health Data of 500,000 Patients. Healthcare IT News.

Serwin, A., Meshulam, D.R., Javanshir, L. (2022). US Senate Unanimously Passes the Strengthening American Cybersecurity Act. DLA Piper Publications- Cybersecurity Law Alert.

Siwicki, B. (2017). Vendor Error Causes Major Patient Record Leak at New York Hospital. Healthcare IT News.

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.

United States Congress. (2022). S.3600 - Strengthening American Cybersecurity Act of 2022.

United States Congress. (2022). H.R.5440 – Cyber Incident Reporting for Critical Infrastructure Act of 2021.

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

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

U.S Health and Human Services. (n.d.). Top 10 Tips for Cybersecurity in Health Care. HealthIT.gov. (Accessed 10/3/2022).

Uzialko, A. (2022). Connected Medical Device Security. Business News Daily.

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.