akerman

Blog Post

Providers: Cyberattacks Are Still Coming - Are You Prepared?

March 22, 2021
By Kirk S. Davis and Danielle C. Gordet

Cyberattacks against healthcare providers accounted for 79 percent of all reported data breaches in 2020 (see here). The U.S. Department of Health and Human Services' (HHS) Office of the Assistant Secretary for Preparedness and Response (ASPR) responded last month by releasing a comprehensive guide to protect providers against this growing vulnerability entitled "Healthcare System Cybersecurity Readiness & Response Considerations" (ASPR Report).

The goal of the ASPR Report is to help providers understand what must occur before, during, and after a large-scale cybersecurity incident. We have provided below a brief overview of the major strategies discussed in the ASPR Report that various types of healthcare facilities can use for a range of cybersecurity incidents. The key points of the report can be summarized by three key concepts: *Think, Remember, and Anticipate*.

Think

According to the ASPR Report, providers must think about all the potential vulnerabilities within facilities and evaluate them. These actions will help providers prepare for a cyberattack and mitigate the harm when—not if—an attack occurs:

Related People

Kirk S. Davis
Danielle C. Gordet

Related Work

Data Privacy and Security
Healthcare
Healthcare Fraud and Abuse
Hospitals and Health Systems

Related Offices

Miami
Tampa

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Visit this Akerman blog

- ***Cybersecurity Readiness***: Ensure IT and leadership teams plan and execute routine evaluations of the facility and departments to understand potential exposure to risk.
- ***IT Evaluations and Assessments***: Assess vulnerabilities and prioritize the impact the assessment has on the provider's business functions. Providers should conduct the Business Impact Analysis (BIA), which identifies mission-critical functions that must be prioritized during recovery efforts after a breach.
- ***Routine Mitigation***: Have patch management processes in place that are able to scan for "patches" within the network and quickly address the weaknesses. "Investment in data backup and redundancy across the IT environment, including external mirroring, is essential for protecting vulnerable systems."
- ***IT Incident Planning***: Understand the threats used to target vulnerabilities within healthcare systems by staying up-to-date on recent attacks. It is also important to have an incident response plan that providers practice and update regularly.
- ***Downtime Scenarios***: Prepare a downtime plan, which includes various workflows and the responsibilities of team members, and ensure downtime guidance is easily accessible to all staff. Periodic downtime exercises and drills should be performed as their "outcomes will identify any gaps in readiness and key weaknesses in response and recovery efforts. Careful planning for downtime will save time while in the midst of a cyber event where resources are maxed."

Remember

The ASPR Report indicates that providers must remember the steps they took to prepare for a cyberattack to anticipate exactly what they will need to do in the first moment that a cyber incident is suspected.

- ***Incident Command Principles***: The Incident Management Team (IMT) should determine the appropriate scope of their response to an event, including knowing what threshold will trigger a system shutdown.
- ***Workforce Resilience***: Ensure procedures are in place to redistribute workload throughout the facility in the event that reallocation of resources is necessary to aid in recovery efforts.
- ***Personnel Adjustments***: Make personnel adjustments to ensure that employees who are unable to work due to impact on computer systems can assist with other areas in the facility.
- ***Operational Considerations***: Ensure processes are consistent across departments and facilities to avoid discrepancies in record keeping and to ensure quality of care.
- ***Response Downtime Procedures***: Departments should already have downtime forms easily accessible to ensure that staff know what is expected of them.
- ***Communication/Information Sharing***: Ensure information is shared clearly and consistently during the incident. For example, initiate a communication plan to manage messaging.
- ***Safety Considerations***: Safety should be monitored, including conducting routine checks in patient care areas to identify areas for improvement.

Anticipate

The length of the recovery process will depend on the severity of the attack. However, providers should anticipate implementing the following processes once they confirm that the attack is no longer occurring:

- ***Financial Recovery:*** Collect financial data early "to ensure the integrity of the cycle from patient registration to claims processing, and collection of payments."

- ***Demobilization***: Define the criteria which will be used to determine when the incident is over and which steps to take at that time.

Getting Started

The task of putting cybersecurity measures in place may seem daunting; however, it is better to plan for these types of attacks now rather than be faced with confusion when the situation arises. In the face of a cybersecurity attack, providers must act quickly and therefore need to be prepared. ASPR has put together various checklists to help providers get started. These checklists include a Hospital Downtime Operations Checklist, a Cyber Incident Response Checklist, a Hospital Downtime Preparedness Checklist, and a Cybersecurity Incident Restoration Checklist. There are also a wide variety of additional resources available. For example, Digital Hands published a playbook, "How to Prevent & Respond to Ransomware Attacks: A Cybersecurity Playbook for Hospitals," which outlines strategies to prevent cyberattacks, the latest tools and technology that can assist with prevention efforts, and what must be done following an attack.

Think, Remember, Anticipate. Cyberattacks are occurring more frequently than ever before. Providers who don't take the actions discussed in this post sooner rather than later will be left vulnerable to attacks and to their aftermath. To avoid cyberattacks and mitigate their harm, preparation is key. The resources discussed above and consultation with health law counsel can help providers determine which measures to implement to best protect their facilities. With the increasing likelihood of cyberattacks and their potential for significant harm to healthcare facilities, the time to prepare is now.

---

administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.