PSNet
PATIENT SAFETY NETWORK

Cybersecurity and How to Maintain Patient Safety

March 27, 2024
Pelletreau B, Riggi J, Gale B, et al. Cybersecurity and How to Maintain Patient Safety. PSNet [internet]. 2024.
https://psnet.ahrq.gov/perspective/cybersecurity-and-how-maintain-patient-safety

Introduction

The integration of information technology (IT) in healthcare has become a cornerstone of efficiency and advancement in the last few decades. Interconnected IT systems within healthcare can streamline processes, enhance patient care, and save lives, but they also introduce a complex web of cybersecurity vulnerabilities. Healthcare has increasingly become a prime target for cyberattacks. Many organizations depend heavily on IT for daily operations. Therefore, losing access to IT systems and to the data contained in these systems has dire consequences.

When a health system experiences a cyberattack, the impacts extend far beyond disruptions to workflows, as patient safety can be compromised during a cyberattack. Important procedures may be delayed, clinicians can lose access to vital information such as medical history and allergies, and healthcare workers must make or defer treatment decisions without timely diagnostic imaging and lab results.[1] In addition, patients' private medical and financial information can be stolen and held for ransom or sold on the dark web.

Recognizing the gravity of these challenges, the Department of Health and Human Services (HHS) has initiated federal support and oversight efforts and the Joint Commission has initiated guidelines to mitigate the risks associated with cybersecurity in healthcare. These efforts aim to establish comprehensive frameworks, guidelines, and regulations to safeguard the integrity of healthcare IT systems and, by extension, protect patient safety.[2]

The Nature and Prevalence of Cyberattacks

Cyber attackers gain access to healthcare systems through tactics like phishing, which require a single employee to click on a link within a deceptive email. After the user clicks the link, malware is installed on their work computer and can spread to the whole organization. The attacking entities can then do any number of things to disrupt operations and extort money. A majority of these attacks are from third-party

providers that service healthcare technology providers in other peripheral services around hospitals and health systems. Among the most common and disruptive types of cyberattacks in healthcare is ransomware, which encrypts all systems and critical data, rendering them inaccessible, until a ransom is paid. This tactic not only cripples essential services such as electronic health records (EHRs) and phone lines but also causes clinicians and administrators to make difficult decisions regarding patient care. According to the Federal Bureau of Investigation (FBI), the healthcare industry was by far the most targeted sector for ransomware attacks; 210 attacks were reported in 2022.[3] In a recent survey of 653 IT security staff in U.S. healthcare organizations, more than half (54%) said their organizations experienced ransomware attacks in 2023, and 59% said the attacks had a negative impact on patient care.[1]

A ransomware attack is often paired with data theft, which threatens to compromise the confidentiality and integrity of sensitive patient information. In addition to holding the healthcare IT systems ransom, data thieves threaten to release private health information of thousands of patients unless they are paid. In 2023, 112 million individuals in the United States were involved in a data breach. That number more than doubled from 2022 (46.8 million), according to the HHS Office of Civil Rights.[4]

How to Prevent and Prepare for Cyberattacks

With the increasing rate and complexity of cyberattacks on healthcare, it has never been more important for healthcare organizations to prevent and prepare for attacks. First and foremost, executive leadership teams need to devote time and resources to this concern and build cybersecurity into organizational policies.[5] New policies may involve appointing someone such as a clinical director of cybersecurity who understands both security and clinical work and can oversee cyber-awareness programs, cyber-hygiene (firewalls, etc.), and cyber-incident planning and response. To prevent breaches to your system security, HHS recommends measures such as using a firewall and antivirus software, having strong password requirements, and training staff regularly.[5] Staff training materials should be easily understandable and free of IT jargon, and can be modeled on successful past patient safety interventions, such as the WHO's "My Five Moments for Hand Hygiene" guidelines and "Surgical Safety Checklist."

Aside from prevention, a large amount of work is involved in planning and practicing a response to an attack, including patient safety protection. Starting with a security framework, such as the National Institute of Standards and Technology Cybersecurity Framework or the HHS Health Industry Cybersecurity Practices, will give organizations an overall sense of how to identify, respond to, and recover from breaches.[6,7] To be accredited, the Joint Commission now requires organizations to conduct a hazards vulnerability analysis and maintain a continuity of operations plan, a disaster recovery plan, and an emergency operations plan.[8] The development and practice of these plans will be critical if a cyberattack brings down EHRs and other IT systems. Planning priority should be placed on items that can affect patient safety, such as obtaining and managing allergy and other medication information, and diverting emergency procedures and services to other facilities. Specific downtime procedures could include calling pharmacies to retrieve medication information, using fax machines for medication orders within the facility, using paper charts, and having runners to communicate between units. However, developing these plans is only the first step; they must be practiced regularly with all teams so that everyone knows how to respond

instinctively when an attack hits, and there is full integration between all the departments.[8]

How to Respond to a Cyberattack

When an attack occurs, systems may start to shut down or a message may appear from the attacking group to notify users of the encryption and ransom terms. The procedures in the emergency management plan should activate an emergency response team, and IT may shut down systems to try to contain the breach. The American Medical Association recommends notifying staff as soon as possible about the scope of the attack and what is being done to address it.[9] To greatly improve activation of downtime procedures, offer pre-prepared, quick-reference informational sheets to clinicians and other staff to refresh themselves on emergency procedures such as how to use paper charts, how to collect consent forms, and how to order medication.[10]

Frequent leadership rounding, team huddles, and intra-unit communication can help to keep everyone informed of potential or current patient safety issues.[11] When a patient-safety event occurs, reporting it (whether on paper or in a short email or through another manual method) remains a top priority so leadership can make informed decisions about patient care during the downtime.[11] For the duration of the downtime, staff and leadership should be prepared to make quick and difficult decisions and to work as a team to ensure patient safety and care remains as high quality as possible under the circumstances.

How to Recover From a Cyberattack

When the attack is resolved, either by paying the ransom or by decrypting the files in-house, recovering from a cyberattack is as important as preparing or responding to one. Decrypted files need to be validated, systems need to be checked for full functionality, paper forms need to be entered into systems, and compromised devices need to be replaced.[12] This recovery process can take several months, and heavy attention to detail is needed in these tasks to ensure that patient safety is maintained. For example, when the medication order-entry system comes back online, pending orders may exist that were already filled by a paper order, and clinicians need to ensure no duplicate prescriptions to patients exist.[10]

Finally, it is critically important for the organization to debrief about the event, determine lessons learned, and develop a plan for carrying out action items. These steps can help the organization prevent, prepare for, respond to, and recover from cyberattacks much more quickly and effectively in the future and, ultimately, better protect patient safety.

Conclusion

Interconnected IT systems in healthcare improve patient safety on a daily basis, but they create risks to patient safety in the event of a cyberattack. The dramatic rise in disruptive cyberattacks in recent years should spur all healthcare organizations to prepare thoroughly for such an attack. Government and accrediting organizations such as HHS and the Joint Commission increasingly emphasize the significance of cybersecurity and acknowledging its pivotal role in ensuring the integrity of patient care. Some best

practices to ensure patient safety include dedicating resources to cybersecurity and clinical continuity, detailed planning and practice for downtime, and debriefing after an attack. By actively responding to regulatory guidance and investing in preventive measures, the healthcare industry can build a resilient system that not only safeguards patient information but ensures uninterrupted and secure patient care in the digital age.

References

1. Ponemon Institute. *Cyber Insecurity in Healthcare 2023: The Cost and Impact on Patient Safety and Care*. Proofpoint; 2024. Accessed February 12, 2024. https://www.proofpoint.com/us/resources/threat-reports/ponemon-healthcare-cybersecurity-report

2. U.S. Department of Health and Human Services Administration for Strategic Preparedness & Response. *Healthcare Sector Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services*. Department of Health and Human Services; 2023. Accessed February 12, 2024. https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

3. Southwick R. FBI: healthcare hit with most ransomware attacks of any other sector. Chief Healthcare Executive. Published March 24, 2023. Accessed February 11, 2024. https://www.chiefhealthcareexecutive.com/view/fbi-healthcare-hit-with-most-ransomware-attacks-of-any-critical-sector

4. McKeon J. This year's largest healthcare data breaches. HealthIT Security. Published December 26, 2023. Accessed February 11, 2024. https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches

5. HealthIT.gov. Top 10 tips for cybersecurity in healthcare. Accessed February 11, 2024. https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

6. National Institute of Standards and Technology. Cybersecurity framework. Accessed February 11, 2024. https://www.nist.gov/cyberframework

7. U.S. Department of Health and Human Services HHS 405(d). Health industry cybersecurity practices: managing threats and protecting patients (HICP 2023 Edition). Accessed February 11, 2024. https://405d.hhs.gov/information

8. The Joint Commission. Preserving patient safety after a cyberattack. *Sentinel Event Alert.* Issue 67. Published August 15, 2023. Accessed February 11, 2024. https://www.jointcommission.org/-/media/tjc/newsletters/sea-67-cybersecurity-7-26-23-final.pdf

9. American Medical Association. Guidelines for developing EHR downtime procedures. Accessed February 11, 2024. https://edhub.ama-assn.org/data/Journals/steps-forward/937327/10.1001stepsforward.2017.0017supp3.docx

10. Massachusetts General Hospital Center for Disaster Medicine. *Hospital Preparedness for Unplanned Information Technology Downtime Events: A Toolkit for Planning and Response*. MGH Center for Disaster Medicine; 2018. Accessed February 11, 2024. https://www.massgeneral.org/assets/mgh/pdf/emergency-medicine/downtime-toolkit.pdf

11. State University System of Florida Board of Governors Healthcare Education Medical Professional Liability Company. *Patient Safety Guidance for Electronic Health Record Downtime: Recommendations of the Electronic Health Record Downtime Task Force*. AMC PSO; 2017. Accessed February 11, 2024. https://flbog.sip.ufl.edu/wp-content/uploads/2019/11/AMC-PSO-EHR-Downtime.pdf

12. Long S. The cyberattack: from the POV of the CEO. *Hancock Health*. Published January 19, 2018. Accessed February 11, 2024. https://www.hancockhealth.org/2018/01/cyber-attack-pov-ceo/