CONVENING LEADERS FOR EMERGENCY AND RESPONSE

Strategies for Preparing for and Navigating Cyberattacks in Health Care

TIP SHEET

With the rise of cyberattacks in health care, hospital and health system leaders are facing an unprecedented threat to their organizations' security, potentially putting sensitive data systems at risk and impacting employee safety and patient care. These breaches can lead to compromised patient and employee data, disrupt critical health care operations and delay essential patient care.

This tip sheet offers strategies and examples from the field on preparing for and navigating cyber incidents.

Key Strategies and Considerations

MANAGE ONGOING PARTNERSHIPS WITH CROSS-SECTOR AGENCIES

STRATEGY Collaborate with critical partners and third-party vendors at the local, regional and federal levels to identify and mitigate vulnerabilities in existing digital systems.

EXAMPLE Atlantic Health System consistently engages with the local FBI field office as well as digital vendors to monitor and mitigate emerging cybersecurity threats.

> "A cyberattack is a crime against humans. Cyberattacks are a crime against our patients."
>
> Brian Gragnolati
> President and CEO, Atlantic Health System

FOSTER A CULTURE OF CYBER PREPAREDNESS

STRATEGY Implement a top-down approach to prioritizing cybersecurity, beginning with board members and C-suite executives.

EXAMPLE Atlantic Health System identifies cybersecurity as a top risk for its organization. As a result, the board receives regular updates on emerging threats and mitigation efforts underway to strengthen cyber preparedness.

STRATEGY Educate, train and equip the IT team to recognize initial signs of a cyberattack, which would minimize the ramifications if an attack occurs.

EXAMPLE University of Vermont Medical Center has implemented a continuous monitoring strategy that equips the IT team with advanced analytics tools to identify and mitigate the initial signs of cyberattacks, minimizing potential damage.

American Hospital Association
Advancing Health in America

ENSURE LEADERSHIP TRANSPARENCY

STRATEGY Provide regular and timely updates to key community stakeholders about cyber incidents, including information on the impact and response progress.

EXAMPLE After a 2020 cyberattack, leaders at University of Vermont Medical Center appeared frequently on local news outlets to inform the community about the health system's response to the attack and explain how services would continue in the immediate aftermath.

> "I encourage organizations to make a department-by-department cyber disaster [response] plan."
>
> Christian Dameff, M.D.
> Medical Director of Cybersecurity
> University of California San Diego Health

USE A MULTIDISCIPLINARY APPROACH TO PREPARE FOR A CYBERATTACK

STRATEGY Ensure a cyber response plan accounts for the potential impact on all aspects of the organization — financial, operational and clinical.

EXAMPLE University of California San Diego Health engages leaders across departments during cyber preparedness planning to consider financial, operational and clinical implications and establish downtime procedures.

STRATEGY During cyber preparedness planning, engage employees across departments to establish effective downtime procedures such as paper charting, writing out pharmaceutical orders and manually filing lab records.

EXAMPLE Following a cyberattack in 2020, University of Vermont Medical Center used walkie talkies to communicate critical lab results to unit floors and stored all lab results in filing cabinets while its electronic health records system was offline.

Watch the moderated discussion on cyberattacks in health care, part of the CLEAR Crisis Leadership Video Series:
youtube.com/watch?v=ztnewBQYrGg

For additional resources, tools and guidance related to emergency preparedness and response, visit www.aha.org/aha-clear.

Presented as part of Cooperative Agreement 5 HITEP210047-03-00, funded by the Department of Health and Human Services' Administration for Strategic Preparedness and Response (ASPR). The Health Research & Educational Trust, an American Hospital Association 501(c)(3) nonprofit subsidiary, is a proud partner of this Cooperative Agreement. This publication is solely the responsibility of the Health Research & Educational Trust and its partners and does not necessarily represent the official policies or views of the Department of Health and Human Services or of the Administration for Strategic Preparedness and Response. Further, any mention of trade names, commercial practices, or organizations does not imply endorsement by the U.S. Government.