Hospital Leadership:

Can You Answer These 5 Questions About Your Cybersecurity Incident Response Preparedness?

Perhaps no sector has more at stake, or is more targeted, when it comes to cybersecurity than healthcare and life sciences. Now more than ever, hospital leadership teams must be actively involved in their cybersecurity incident response planning efforts so cyber attacks can be handled effectively with limited financial, operational, legal and reputational damage. Answering the questions below will put your leadership team on the right track toward enhancing your cybersecurity preparedness posture.

70%

of healthcare and life sciences leaders surveyed said their organization experienced a cybersecurity incident in the last 12 months.*

For hospital leadership, to be adequately prepared means to respond when incidents arise and have a tried and true, multistakeholder cybersecurity strategy in place.

*According to FTI Consulting's U.S. Healthcare & Life Sciences Industry Outlook 2023 survey

Do you understand your organization's cybersecurity maturity?

Conducting a cybersecurity maturity assessment to identify critical gaps and risks in your organization's existing infrastructure can lead to the development of an effective roadmap to guide organizational cybersecurity investment decisions. An effective roadmap can also minimize the likelihood of an incident and the impact to reputation in the event of one. Having experts in place that know your organization, stakeholders and values is critical to quickly navigating the immediate and long-term aftermath of a cyber incident.

Who has decision making authority in the incident response process?

It is important to identify accountabilities to be better prepared to handle post-incident recovery activities. Clear ownership is recommended across critical workstreams, including: containment, restoration and recovery, forensic investigation, legal and regulatory response and internal and external communications. Knowing who has decision making authority in critical aspects of the incident response process, and who is leading corresponding workstreams, will enable the swift and decisive action that is required to effectively manage an incident.

Is your staff up-to-date on organizational cybersecurity policies?

The prevalence of cybersecurity incidents presents an opportunity to refresh staff on your organization's existing data retention, cybersecurity and social media policies, especially those that are healthcare or HIPAA specific. Reinforcing policies through periodic training and awareness programs consistently builds cybersecurity hygiene across all organization levels. The effectiveness of individual diligence can be multiplied by having a dedicated team in place to monitor for early signs of incidents, including insider threats and misinformation campaigns.

How will you communicate with key stakeholders in the event of a significant cybersecurity incident?

In the wake of a cybersecurity incident, organizations will be pressed to communicate quickly to provide guidance to staff and to establish confidence in customers, partners and patients regarding restoration progress and the availability of critical services. However, attacks often render typical methods of communications – including corporate e-mail – inaccessible. In advance of a serious issue, organizations should establish out-of-band communications solutions for reaching stakeholders and streamlining internal processes for developing, approving and disseminating messages.

Additional Resources

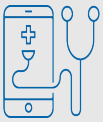
PODCAST

Anticipating and Addressing Emerging Cybersecurity Threats

VIDEO

Cybersecurity Communications Hygiene for Healthcare Leaders

ARTICLE



The Internet of Medical Things and Cybersecurity Risk

ARTICLE

A Presidential 'Prescription' for Hospital Cybersecurity

What third parties have access to your organization's systems or data, and has their cybersecurity maturity been evaluated?

Many healthcare organizations rely on vendors, suppliers and contractors to assist with their day-to-day operations, and these third parties are often granted access to the organization's network or data. While outsourcing can create efficiencies, organizations need to understand and plan for potential impacts if a connected entity suffers a cybersecurity incident. This can be accomplished by determining what vulnerabilities the organization has limited control over, identifying actions to mitigate these risks pre-incident, and implementing a plan for what to do if a third party is hit with a cyber attack.

MATT CHEVRAUX
Managing Director
Cybersecurity
+1 202 394 5480
matt.chevraux@fticonsulting.com

JAMIE SINGER
Managing Director
Cybersecurity & Data Privacy Communications
+1 847 414 1377
jamie.singer@fticonsulting.com