THE ROLE OF LEADERSHIP IN DATA BREACH DEFENSE

HOSPITAL EXECUTIVES MUST BE INVOLVED IN DATA BREACH DEFENSE. HERE'S HOW THEY CAN FACILITATE ACTIVE ENGAGEMENT WITH IT/IS TEAMS.

Senior executive leaders play a critical role in data breach defense. While they are more familiar with clinical operations than IT staff, they are also responsible for overseeing hospital systems such as EHR/EMR, billing, telemedicine, radiology, and others. These executives are primarily concerned with patient safety and delivery of high-quality care. These and other factors, such as HIPAA compliance, institutional reputational, and financial consequences like from regulatory fines and lawsuits are also directly impacted by cybersecurity. That's why it's crucial for hospital leadership to be involved in data breach defense. Here are ways that executives can get more involved.

JOINT PLANNING

Hospital executives must work closely with IT/IS teams to develop an incident response plan (IRP) that includes clear policies and procedures for preventing data breaches. Executives need to ensure that IT implements standard security measures, such as multi-factor authentication (MFA), data encryption, patch management, and employee training. However, IT needs executive support to overcome obstacles like resistance to MFA, securing legacy systems, and ensuring consistent employee training to prevent phishing attacks.

DATA BREACH PREVENTION

Effective prevention requires executive oversight. Hospital leaders can help IT/IS by ensuring staff understands the importance of MFA and that legacy systems are properly secured. Executives should also be involved in differentiating between “technical” and “business” data breaches. A technical breach refers to unauthorized access to data, while a business breach involves organizational or human error. Identifying the nature of a breach helps ensure the right response is enacted quickly.

INVESTIGATION AND DECLARATIONS

When a data breach is detected, immediate involvement from hospital executives is crucial. Rapid decisions must be made regarding the activation of the IRP and breach disclosure protocols. This often requires close collaboration between IT/IS teams, legal counsel, hospital leadership, and external experts. Hospital executives are tasked with assessing the breach’s scope and impact and ensuring timely and appropriate notifications are made to affected individuals, regulatory bodies, and any other necessary stakeholders.

RESPONSE AND CONTAINMENT

Containing the breach is crucial to minimizing data loss. This involves stopping the data exfiltration and preventing the breach from spreading to other systems. A key challenge for hospital leadership is deciding which systems should be shut down or isolated during the containment phase. The typical response from IT teams is to disconnect compromised systems from the network, but decisions must balance security with operational needs. Hospital executives may need to amend the IRP quickly in response to business pressures and legacy system complexities.

COMMON UNDERSTANDING OF DATA BREACH ACTIVITY

Hospital executives and IT/IS teams should share a common understanding of the breach’s status at the hospital or clinic level. This shared perspective is crucial for avoiding confusion and delays during response. While IT/IS may need time to investigate, executives should be informed early about potential issues to ensure swift decision-making.

SPECIFIC DATA BREACH EXERCISES

Regular breach exercises, focused on detection, investigation, declarations, and containment, help executives and IT/IS teams work together more effectively during a real incident. These exercises can test the IRP, highlight gaps, and foster a collaborative approach to breach management.

ESSENTIAL CONSIDERATIONS

Improving communication and collaboration between hospital executives and IT/IS staff is essential in defending against data breaches. By fostering a common understanding of breach activity and regularly practicing breach detection and response, hospitals can strengthen their defense posture.

Celerium's Compromise Defender® solution helps executives and IT teams collaborate more effectively and manage breaches with greater efficiency. It improves collective awareness and enhances visibility of potential threat activity through reporting and notifications. Automated detection helps alleviate the workload of IT teams, and manual and automated containment functions enable appropriate actions. For more information on Celerium's data breach defense program, **visit our website** or contact us at **info@celerium.com**.

ABOUT CELERIUM

Celerium® powers active cyber defense solutions to help protect organizations and communities from increasing cyberattacks. With a rich 16-year history of facilitating cyber threat sharing for critical industry sectors and government agencies, Celerium is an established leader in providing innovative cybersecurity solutions, with solution directions based on the evolving needs of the industry.

Learn more at **www.Celerium.com** and follow us on X at **@CeleriumDefense**

CELERIUM.com