COMPROMISE DEFENDER®

ENGAGING HOSPITAL LEADERSHIP FOR DATA BREACH DEFENSE

CELERIUM.com

INTRODUCTION

Improving organizational engagement is paramount in the face of increasing data breach attacks. This engagement must extend beyond the IT/IS department and involve hospital executive leadership given the enterprise-wide risk and responsibility. This article will highlight the importance of hospital executive involvement in data breach defense and provide strategies for effective engagement.

THE NEED FOR HOSPITAL EXECUTIVE INVOLVEMENT IN DATA BREACH DEFENSE

Hospital executives, including CEOs, COOs, and CFOs, as well as clinical executives play a critical role in data breach defense. These executives are more familiar with hospital than IT/IS staff. They are also more focused on selected hospital systems such as:

- EHR/EMR, Health Information Exchange (HIE),
- Financial,
- Telemedicine,
- Laboratory,
- NICU/Labor,
- Nursing Station,
- Radiology, Imaging,
- Nutrition, and Pyxis

Moreover, hospital executives have more responsibility for HIPAA regulatory compliance and possible data breach disclosure obligations. They are also more concerned about patient safety, reputational damage, and financial impacts such as regulatory fines and class action lawsuits. All functions of a hospital are impacted by a cybersecurity breach, so the C-suite team needs to be directly involved in breach defense.

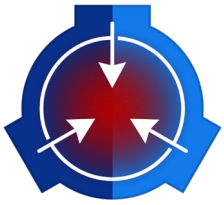
PHASES OF DATA BREACH DEFENSE

Joint Planning Stage: This involves the creation of an incident response plan, key systems, policies, and procedures relating to data breaches. Hospital executives, including the C-suite and clinical operations executives, need to ensure that the IT/IS department implements standard prevention measures such as multi-factor authentication (MFA), data encryption, patch management, and awareness training. However, IT/IS often needs guidance and help from executives to overcome challenges such as employee resistance to MFA, implementing prevention measures on older and fragile legacy systems, and ensuring all employees participate in recurring awareness training to reduce the impacts of phishing attacks.

Data Breach Prevention Measures: Implementing these measures is crucial but often requires executive oversight. For example, executives can help ensure that all employees understand the importance of MFA and that legacy systems are properly secured.

While IT/IS typically handles detection and response, hospital executives need to be involved in distinguishing between "technical data breaches" and "HIPAA or regulatory data breaches." Technical data breaches involve determining if data is being lost to a malicious destination, which can be problematic due to false positives. Executives can help clarify whether a data breach is technical or regulatory, ensuring timely and appropriate responses.

Data Breach Investigation and Declarations: Even if IT/IS has confirmed malicious activity, hospital executives need to be involved in determining whether to activate an internal incident response process and prepare to submit Data Breach Disclosure documents to HHS/OCR and other appropriate federal or state regulatory organizations. These determinations can be complicated and require the creation of teams involving IT/IS, Hospital Leadership, and outside experts from Legal, Insurance, and other organizations.



Data Breach Response (Containment): Often, in discussions about what happens after a data breach has occurred, the conversation is about the response in terms of the broad incident response plan. However, focusing on the front end of incident response (containment) is essential in a data breach where time is of the essence. Containment has two different dimensions. First, stopping the bleeding of breached systems is necessary to prevent any further loss or exfiltration of data to malicious sources for those systems. Then, stopping the spread of the bleeding is vital in preventing other systems from future data breach activity.

A major dilemma for hospital leadership is which systems should be shut down during containment. A common IT/IS response to stopping the bleeding is called isolation. This process often involves disconnecting infected systems from the network to stop the spread of the bleeding. In concept, the IR plan may have defined the systems that can and should be shut down. But that IR plan may be problematic for several reasons:

- Out of date, changing scope
- Shadow IT systems
- Legacy systems
- Business pressures that are felt within the first 24-48 hours which may require a change from the IR plan
- But who makes these decisions?
    - Internal IT organization?
    - An outside Incident response firm?
- Is hospital executive management delegating or abdicating these crucial decisions to IT or to external IR firms?

STRATEGIES FOR ENGAGING HOSPITAL EXECUTIVES AND IT/IS STAFF

PROVIDE A COMMON UNDERSTANDING & VIEW OF DATA BREACH ACTIVITY STATUS

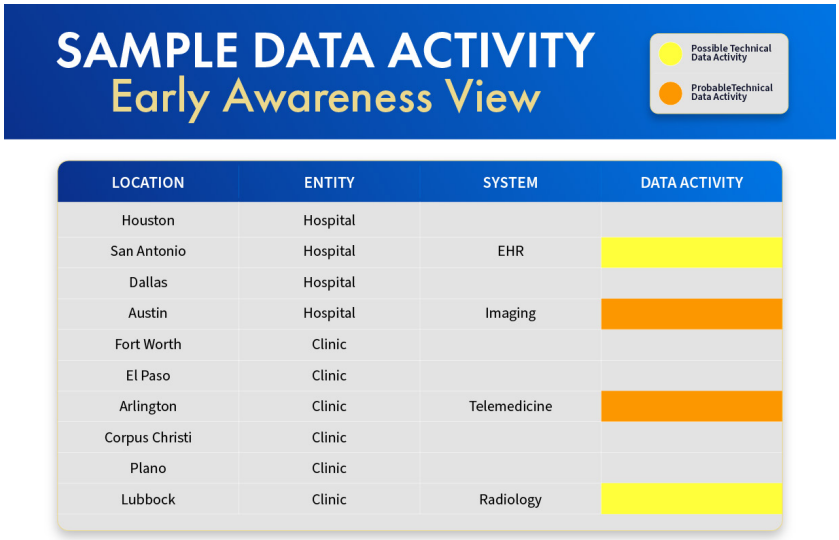
If possible, hospital executives and the IT/IS organization should have a common operating picture of data breach activity at the hospital or clinic level as well as the underlying health systems (above) that normally hold ePHI data. From an executive and business point of view, this is not about the technical world of SIEMS, IP addresses, or threat hunting. Both teams having the same view can avoid confusion and delays. The goal is to enable organizational synchronization between IT/IS and hospital executives. Certainly, it's appropriate for IT/IS to have some time to analyze most problems before business executives are informed. Yet, given how overloaded most IT/IS organizations are, a key issue is how much time should elapse before hospital executives get informed. Should there be an early awareness approach to give hospital executives a heads-up regarding potential issues while IT/IS is still investigating?

Specific Data Breach Exercises: Cybersecurity exercises normally focus on handling security incidents. They are not focused on the earlier planning or prevention stage, although exercise outcomes could influence planning and prevention measures. Often, exercise participants will encounter issues (called injections) that an IR plan may not cover. Specific data breach exercises provide a formal process to push hospital executives and IT/IS staff to be much more agile and hopefully collaborative. For data breach exercises, four appropriate elements could be:

1. **Data Breach Detection:** Dealing with the vagaries and uncertainties of detection. Understanding and thinking through the evolution of confidence, certainty, knowledge
2. **Data Breach Investigations:** Understanding which investigations need to be implemented by IT and which require help beyond IT.
3. **Declarations:** As a result of the above investigations, it is often appropriate to have selected formal declarations of data breach status for internal or external purposes. Specialized teams would normally create a more formal declaration:
    a. **Internal Declaration:** Activation of an internal IR plan.
    b. **External Declarations:** Alerting patients, partners, HHS and media (if more than 500 ePHI records have been stolen), formal disclosures to other federal regulators, and to potential state regulators.
4. **Response (Tactical Containment):** Making the following, very difficult business decisions:
    a. Which systems to isolate or shut down in the face of a data breach.
    b. When isolated or disconnected systems can be brought back on-line.
    c. When isolated or disconnected systems may need to be brought back online even if technical safety measures (forensic work, prevention, etc.) are not yet finished.

HOW CELERIUM HELPS FACILITATE EXECUTIVE ENGAGEMENT FOR DATA BREACH DEFENSE

Celerium powers data breach defense that is automated, effective, and engages all levels of the organization – with an emphasis on providing early awareness of potential technical data breach activity through executive-level dashboards and reporting.



LOCATION	ENTITY	SYSTEM	DATA ACTIVITY
Houston	Hospital		
San Antonio	Hospital	EHR	
Dallas	Hospital		
Austin	Hospital	Imaging	
Fort Worth	Clinic		
El Paso	Clinic		
Arlington	Clinic	Telemedicine	
Corpus Christi	Clinic		
Plano	Clinic		
Lubbock	Clinic	Radiology	

Compromise Defender® facilitates visibility into potential breaches for IT/IS teams and hospital executives. The Early Awareness report provides a community view into specific systems at various locations so teams can take action to investigate further and make decisions.

The solution's automated detection and containment tools also can reduce the overall IT/IS burden. Server-based reporting enables monitoring of key systems, and the powerful notification and alerting system keeps team members informed and aware of potential threats.

Celerium is currently offering a no-cost data breach defense program for health care organizations, leveraging the powerful Compromise Defender solution. For more information on our data breach defense program, visit the Celerium 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