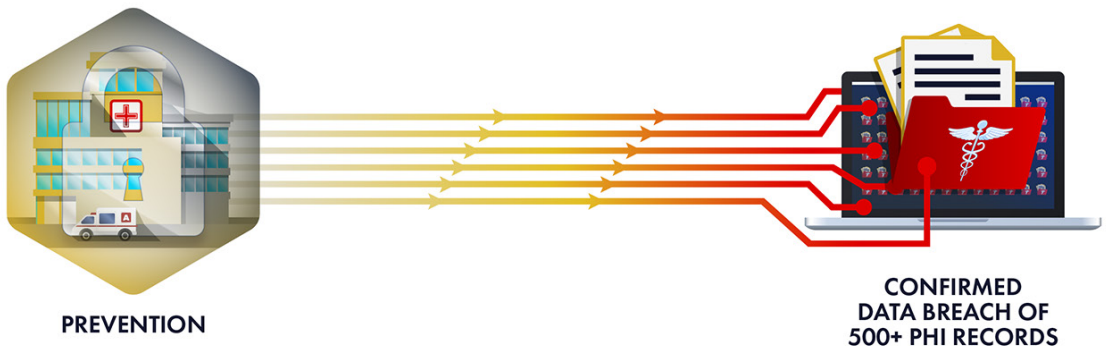
IMPROVING HOSPITAL EXECUTIVES' EARLY AWARENESS OF DATA BREACHES

INTRODUCTION

Hospital executives face a critical issue in mobilizing organizational focus on data breach defense. Instead of focusing only on prevention before a breach and response after a data breach has occurred and is reportable to HHS OCR, hospitals should consider the time in between – to evolve an institutional focus on proactivity by understanding Early Awareness of possible data breach activity.

THE CHALLENGE OF EARLY DETECTION

Understandably, most attention today is on prevention measures. However, when a data breach occurs, and IT or IR processes formally determine that more than 500 ePHI records have been stolen, the organization starts the 60-day clock to submit a Data Breach Disclosure document to HHS/OCR. The dilemma, per seven years of IBM research, is that the average data breach detection time can take months—possibly as long as 6.9 months (about 200 days).



THE NEED FOR PROACTIVITY

Common high-level accusations of hospitals that experience data breaches are that there was a failure to protect patient data adequately along with insufficient investment in cybersecurity infrastructure.

1. **Failure to Implement Proactive Prevention Measures**: Failure to implement MFA, data encryption, patch management, and awareness training could be considered a failure to implement proactive prevention measures.
2. **Failure to Implement Monitoring Systems**: Monitoring systems before a breach is vital because threat actors can often breach systems despite prevention measures. Implementing detection mechanisms for possible data breach activity can provide a proactive awareness (also known as "left of boom" insights).

EXECUTIVE LEVEL AWARENESS VIA EXECUTIVE DATA BREACH DASHBOARDS

The IT organization needs to understand the technical dimensions of possible data breach activity. Many hospital CEOs and other executives also feel pressure to be more proactive regarding data breaches. A set of summary and high-level Executive Dashboards needs to be created so that executives can understand possible data breach activity.

EXECUTIVE DATA BREACH DASHBOARDS: INDIVIDUAL BENEFITS FOR A HOSPITAL CEO

1. **Personal Heads Up:** A personal heads-up before a formal data breach is declared internally can enable a CEO to better understand the situation and associated risks.
2. **Demonstrate Personal Responsibility:** CEOs can demonstrate personal executive responsibility and proactivity.

INSTITUTIONAL BENEFITS OF ORGANIZATIONAL EARLY AWARENESS AND PROACTIVITY

1. **Develop Organizational Responsibility:** Implement a system that mobilizes and synchronizes hospital executives and IT staff around common data breach warnings.
2. **Implement Early Tactical Response:** Early visibility about potential breaches can enable early tactical response, potentially lowering the probability of a full-blown data breach.
3. **Improve Organization Agility:** Improve organizational maturity and competence when addressing ever-evolving threat actor attacks.
4. **Involve Business Executives and Managers:** Involve business executives and managers in proactive data breach defense.
5. **Implement Effective Solutions:** Utilize data breach defense programs that provide dashboards for executives and IT staff.

ESSENTIAL CONSIDERATIONS

It is important to emphasize that early awareness reports of potential data breach activity do not replace thoughtful and measured analysis and confirmation by IT and/or by formal IR processes.

It is also important to find the right strategic partner to help with early awareness of potential data breach activity. How does the partner monitor for potential threats? Does the partner's solution put extra burden on your IT team, or does it leverage automation to reduce the IT burden? Is the solution intrusive, and what data does it touch? Does it require onerous setup or is it engineered to be set up quickly and efficiently?

Celerium can be a strong strategic partner for early awareness of potential data breach activity through its Compromise Defender® solution. The SaaS solution is a cloud-based automated and integrated approach that is optimized for speed, scalability, and automated response actions such as blocking, containment, and notifications.

The bottom-line result is that Compromise Defender Defense provides the muscle to perform the big data analysis for data breach defense, reducing the burden on your IT team. It sets up quickly and does not require installation of new hardware, software, or intrusive black boxes. And it does not touch any ePHI or other sensitive data.

For hospital executives, Celerium's solution includes a powerful reporting engine that provides summary and detail insights. Summary dashboard views show which hospitals or clinics may be experiencing data breach activity, and which hospital systems (e.g., pharmacy, surgery) are affected. There are also detailed technical and network views for IT staff. It also enables notifications of unauthorized network and potential data breach activity to be established for selected IT and IT security teams, or hospital executives.

CONCLUSION

In an era where data breaches are increasingly sophisticated and frequent, it is imperative for hospital executives to prioritize early awareness of potential data breach activity. This proactive approach not only fortifies the organization's defense mechanisms but also cultivates a culture of accountability and preparedness at all levels. By leveraging tools such as Executive Data Breach Dashboards, leaders gain critical insights that enable timely and informed decision-making, ultimately enhancing the organization's resilience against cyber threats.

Partnering with a strategic ally like Celerium further amplifies these efforts. Their Compromise Defender® solution offers a seamless, automated approach to monitoring and response, ensuring that hospital executives and IT teams can swiftly identify and address potential vulnerabilities without the burden of extensive manual oversight. This solution not only enhances operational efficiency but also safeguards patient trust and data.

Ultimately, the commitment to improving early awareness of data breaches will not only safeguard patient data but also empower hospital executives to lead their organizations confidently into the future, equipped to tackle the challenges of an increasingly complex digital landscape.

ADDITIONAL INFORMATION

Celerium offers a no-cost data breach defense program for healthcare organizations, leveraging expertise from providing security solutions to the Department of Defense. **The Compromise Defender** solution includes powerful data breach dashboards and notifications for hospital executives and IT staff, along with manual and automatic containment functions.

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