Cybersecurity Breach-
Incident Response True Cost$

Healthcare providers are required to follow HIPAA rules to protect patients' PHI, but in Q1/2017 more than 88 breaches occurred (http://ocrportal.hhs.gov) . They varied from hacking/IT, improper disposal, email, loss, theft and unauthorized access. The goal of a physician organization or provider's organization is to protect the business – compliance is required and security is the goal.

When a breach happens, there is a cost involved.
The costs are:

- Direct costs – technical investigation, breach notification, regulatory compliance, public relations, legal fees and the costs to improve cyber security measures
- Indirect costs – Public Relations, Loss of revenue, Time to recoup the lost revenue.

Most organizations prepare in advance for a breach.
The preparation includes:

- Inventory of hardware, software, data
- PHI process, stored, protected and the retention
- Implement best practices – access based on need to know, monitor endpoints, risk assessments, etc.
- Have an incident response plan and a team.

The incident response plan includes conducting an assessment with the CISO (Or an external consultant), notifying Insurer, engaging cyber security attorneys, consultants to perform forensics, Public Relations firm, a call center to answer patient inquiries, and remediation services.

The plan includes which legal firm to hire, which consulting firm to hire, etc. Engaging third parties or vendors after a breach is expensive, and depends on their availability.

- What costs they will charge?
- Do the firms have right personnel available to do the work?
- What are the contractual arrangements?
- What resources of the firm are available – Time/availability, physical employee/consultant availability, etc.?

Where will the cost/money come from?
Most provider organization's margins are squeezed either due to payer contracts or shift towards value based care, including MACRA costs.

Yearly budgets include the cost of the cybersecurity, compliance etc. but there is no allocation for an expense in the event of a breach. If a breach happens, where will the money come from to support the incident response plan? Having insurance is fine, but the claim takes substantial amounts of time to process. In the short term the CFO must use either Line of Credit or transfer money from other accounts.

As a CFO/CMO Are you prepared to implement Incident Response Plan? Allocate the costs? Plan for the breach – Resource, time?

At MindLeaf (www.mindleaf.com) we have been protecting patient privacy by ensuring the providers have the right procedures, policies and tools to monitor privacy AND Vendor risk management. MindLeaf and Intel are offering complementary breach security assessment for healthcare organizations.

==========

Author:
Paresh K. Shah