We've Had a Breach: Time to Put That Plan Into Action

Jon Klein JD CHC & Jeff Dover JD CHC

Background

- Started February 23, 2015
- Discovered February 26, 2015
- Malware infection captured a username and password

Insurance

- Insurance only covered 50,000 lives
- 1.5 lives on the server
- 151,626 were accessed
- Total Cost undetermined at this point.

IT Aspects

- 10% increase in traffic
- Database accessible from all IP's
- Database used 24x7

IT Security

- Data is Encrypted at Rest
- AV on all machines
- Root Kits, Crytpo Locker, Trojans are not always detectible by AV and other scanning systems including Windows Defender
- Constant Traffic Monitoring
- AI for abnormal usage

The Fire drill Starts

- Determine source and type of breach
- Cut off access
- Determine how to prevent further intrusion
- Assess immediate risks
- Contact insurance company

The shock wears off

- Determine who is affected
- Plan to notify regulators
- Plan to notify affected Business Associates

Get the Game Plan in Place

- Identify Vendor for Notification
- Work to get notification letter finalized
- Write Scripts
- Write Media Release
- Determine internal points of contacts

Putting the Plan Into Action

- Notify Regulators
- Notify Business Associates
- Notify Staff/Media/Mail Notifications on the same day.
- Make sure your reps to external entities know what they are talking about.
- Give staff the information they need to help
- Update Policies and Procedures

The Plan is Great Until it Goes Into Action

- Leaks
- Returned Mail
- Volume of Calls
- Lawsuits
- Call Center Issues
- Timelines
- Access to Decision Makers
- Access to Data and Information
- Controlling the situation

The Plan In Action Continues

- Too Many Chefs in the Kitchen
- Angry Members
- Maintaining the Chain of Command
- Educating Others

Thank-You!