EGB insurance

Topics we explore when doing a risk assessment for a hospital

This is more of a conversation on each topic than a list of questions.

The goal is to understand the client’s solutions for each topic. We know that there are often many ways to get to a level of defenses and we are flexible in how each client approaches each of these issues.

Topics

- Do you give Phishing education to all your employees?
- Do you give Privacy education to all your employees?
- The process for identifying an incident or event.
- The process for assessing the potential seriousness of this event – litigation, compliance, reputational, or cost
- For those events that are deemed possible serious events, what is their strategy for assembling the team that is going to analyze and respond to it.
    - What skills are on the team?
    - In-house or outsourced?
    - How do they prepare for the possibility of litigation?
- How much of their data is encrypted? To what level?
- What are their policies for BYOD (mobile devices owned by employees or others – as opposed to owned by the client)? What kind of controls are on those machines?
- Does the client have a SOC?
    - If yes:
        - Dedicated or shared?
        - 24/7/365
        - How broad is their ability to react to a possible attack?
        - Who manages it? How big is their team?
        - What percent of the port do they monitor?
    - If no:
        - Do you have APT (Advanced Persistent Threat Management) installed?
        - Do you have SIM (SIEM) installed?
        - Do you have IAM (Identity and Access Management) installed?
        - Do you have DLP (Data Loss Protection) installed?
        - What percent of the port do they monitor?
- How do you test your defenses?
    - Regular penetration testing by outsiders? If yes, how long?
    - Formal Fire Drills designed and supervised by an outside firm?