2016 CLM Annual Conference
April 6-8, 2016
Orlando, FL

"CYBER-ATTACK PREPAREDNESS TOOLBOX"

APPENDIX A
CHECKLIST FOR PERIODIC AUDIT OF EMERGENCY RESPONSE READINESS

Set forth below is a checklist of areas for an Organization to address throughout the year to ensure its readiness for a cyber-event. This checklist is for use by an Organization to ensure an ongoing state of readiness.

1. **Ensure that your emergency response plan remains comprehensive.**
    a. How often: quarterly.
    b. Ensure that the emergency response plan is updated to account for new policies for data management, the development of new business lines, or other significant changes in the Organization.
    c. Ensure that all members of the response team (especially any new team members) understand his or her role in the event of a cyber-attack.

2. **Update contact information for emergency response team.**
    a. How often: quarterly.
    b. Ensure that the emergency response plan has current and up to date contact information for all team members (both internal and external).
    c. Update list to reflect new employees and those who are no longer with the Organization, and to ensure that your list includes current names for outside resources, i.e., contractors, vendors.
    d. Ensure that all team members receive the updated contact information.

3. **Evaluate relationships with business partners and vendors who have access to the Organization's data.**
    a. How often: quarterly.
    b. Evaluate contracts with business partners and vendors to ensure that they are in force.
    c. Ensure that business partners and vendors who have access to an Organization's data are complying with any relevant data protection standards.
    d. Ensure that business partners and vendors are aware of and in compliance with any new regulations or laws that are applicable – include in contracts.
    e. Ensure that a business partner or vendor understands the importance of advising you immediately in the event of a breach.
    f. In order to satisfy HIPAA requirements, an Organization engaged in healthcare business should ensure that business associate agreements are in place.

4. **Evaluate contracts with vendors on the breach team.**
    a. How often: quarterly.
    b. Review contracts with external IT/forensics firm, any data breach resolution partners or other vendors. If necessary, update or renew the contracts.
    c. Evaluate whether your existing contracts are still sufficient in light of any changes to your Organization.

5. **Evaluate insurance coverage.**
    a. How often: annually or at renewal of policies.
    b. Review nature and extent of insurance coverage to ensure its adequacy.
    c. Determine if any changes in your business require new or different insurance coverage.

6. **Evaluate new regulations or laws.**
    a. How often: as enacted or quarterly.
    b. Evaluate any new laws or regulations that have been enacted at the state or national level and make any necessary adjustments to risk management policies.
    c. Update any templates for notification letters that will be used in the event of a cyber-attack.
    d. Do you need to update contact list to add any regulators or government agencies who must be notified of a cyber-event?

7. **Assess status of IT security.**
    a. How often: quarterly.
    b. Consider need for penetration testing by outside forensics expert.
    c. Work with IT department to ensure that appropriate data access controls are in place.
    d. Ensure that the Organization is properly backing up data.
    e. Ensure that the Organization has, in place, appropriate controls for access to data and that employees do not have unfettered access to an Organization's information.
    f. Confirm the proper installation of Organization-wide automation of operating systems and any appropriate updates for software.
    g. Review the automated monitoring of and reporting about systems for gaps in security, and determine whether it is up to date.

8. **Evaluate employees' cyber-awareness.**
    a. How often: annually.
    b. Are appropriate Organization personnel up to date concerning procedures for the protection, preservation and destruction of company data?
    c. Remind employees about the "tricks of the trade" that hackers use, and how to identify the signs of a possible breach or hack.
    d. Ensure that employees understand the importance of reporting a cyber-event or suspected event, and the procedure for doing so.
    e. Remind employees about the importance of regularly changing passwords, and properly securing mobile devices, laptops, etc.