#13

Please complete all the following questions concerning the Information Technology environment within your organization. These questions are intended to be answered by an IT Director (or equivalent professional) with adequate knowledge of the organization's cybersecurity measures and protocols. All questions require completion for Privacy or Security Event Liability coverage. Increased limits will require underwriting review for consideration.

To be considered for a $1M Privacy or Security Event Liability and Expense limit the following must be met satisfactorily:

1. Our staff receive mandatory cybersecurity awareness training at least annually on expectations of staff to recognize common cyber-attacks, such as social engineering and phishing, to report possible cybersecurity incidents or other types of cyber-attacks, and to know who to report cybersecurity issues/problems to.
    a. No, we do not receive mandatory cybersecurity awareness training annually.
    b. Yes, we are required to participate in mandatory cybersecurity awareness training at least annually.
2. Our staff logs in to their web-based email using multi-factor authentication (e.g., receiving a text message to validate log in).
    a. True
    b. False
3. Our critical and sensitive data is backed up, stored and encrypted offline on a different logical or physical network such as a cloud backup to support recovery from a catastrophic cyber incident if required.
    a. True, but our backups are not stored offline on a different logical network location; they are connected to our IT network, and they are encrypted.
    b. True, our backups are offline (in a different logical network) and encrypted.
    c. True, our backups are offline (such as a manual hard drive backup), but they are not encrypted.
    d. False, we do not back up our critical or sensitive data.

To be considered for a $2M Privacy or Security Event Liability and Expense limit the following must be met satisfactorily in addition to the questions noted above:

4. My organization/county has formalized IT and cybersecurity policies and plans that document, for example, guidelines for acceptable use of IT, passwords, reporting of unusual activity (e.g., workstation locking up or not functioning properly), cybersecurity training, and cyber incident response.
    a. We have no documented policies or plans.
    b. We have some documented policies, procedures, and plans, but there are known gaps.
    c. We have a robust, well documented IT and cybersecurity program that is current.
5. Our organization/county requires multi-factor authentication for remote access to our network (both cloud-hosted and on-premises, including Virtual Private Networks (VPNs))
    a. True
    b. False
6. We review our organizations' IT and cybersecurity policies, procedures, and plans at least annually and we make updates/changes based on changes in the organization, the cybersecurity environment, and technology.
    a. True
    b. False
7. In the case of a cybersecurity incident, we report the incident to.
    a. Cyber Insurance Provider
    b. Cyber Insurance Provider and Law Enforcement
    c. Cyber Insurance Provider, Law Enforcement, and Cyber Incident Support Vendors (may include Cyber Forensics, Cyber Legal Support, and other Cyber Incident support)
    d. None of the Above