TOP 10 MISTAKES TO AVOID IN A DATA BREACH SITUATION

Propel Insurance

Your firm has become the victim of a hacker attack or some other data breach situation. Here are ten mistakes you should avoid:

1. Don't act rashly. Collect all of the facts before you respond. Often, the full story ends up being very different from the earliest versions.   Give the IT "first responders" enough time to do the work to fully understand the situation first.

2. Don't just power down your network, it could harm your business and also destroy important data to help determine the extent of the breach. Let your forensics team make that decision.

3. Don't ignore reality or put the problem on the back burner. Alert everyone on your response team as quickly as possible.

4. Don't hire the wrong advisors. Your preferred outside counsel should not represent you in a Data Breach situation if they don't have the appropriate experience. Likewise, don't just hire the first public relations, credit monitoring, consumer notification or forensic advisors that you find at whatever prices they might demand. Take the time to hire well-qualified and strongly-recommended experts at appropriate prices.

5. Don't set false deadlines to accomplish any particular step in the process, at the risk of having to repeat them.

6. Don't notify more individuals than are appropriate, as required by law or to best maintain your firm's reputation.

7. Don't tamper with your files or delete documents that might be subject to discovery in a lawsuit.

8. Don't fail to cooperate with government investigators or regulators. In many cases, counsel will advise that is appropriate to proactively notify law enforcement.

9. Don't just keep loose track of the steps you take. Document everything, in detail, with reasons behind the actions.

10. Don't assume that if you don't make any of the above mistakes you will avoid a lawsuit (or win one).