5 Tips to master ransomware response.

1 Take Ongoing Notes

Make Sure You Include Time Stamps. Getting through an event is your immediate goal. Just as important is the Legal and insurance investigation,a process which may take months or even years. Notes will be critical for that part of the process. include financial decisions (include cost, time & effort at the time of the event, as well as alternative choices).

2 Contact Communication is Key

The Size of Your Company Will Dictate the Number of Communication Channels. Channels may include executive team, all company, clients, 3rd party vendors & satellite offices, not just the-technical staff. Prepare all your employees to have a consistent message.

3 Designate Point-Person

Include the Designations in your Communications. Employees may inadvertently delay your team's process with questions, suggestions, special requests, etc. Someone dedicated to address executive needs or affiliated companies or key departments will allow the rest of your staff to focus on their tasks.

4 Plan Ahead To Prevent Burnout

Ransomware events my take months to resolve. A well-rested team will allow you to continue to provide the service needed. Improper rest can potentially introduce mistakes which may set you back weeks or longer to recover. Having a designated hotel nearby may be necessary.

5 Remind Your Team Not To Make Legal Advice

Answering questions like "is a disclosure required?" "are you doing forensics?", "do we need an attorney?", or "Should we pay the ransom?" could have adverse legal ramifications. This should be part of your internal communications and your point-person designation. Your team can disclose what is being done or what was found, but answering any other questions should always be centralized, both internal to the company and to external parties.