Cyber Incident? Hacked? Breached?

Follow These 10 Important Tips:

1. For the best chance at success, call VESTIGE early: 1-800-314-4357

   Investigating the device(s) on your own will likely trample over valuable evidence and artifacts that may be useful in the investigation. This could make it impossible or at least more costly in your matter.

2. Refrain from turning the device off as it may lose crucial information in memory -- such as a virus or decryption keys.

3. Chances are attackers have been in your system for a long time -- up to 7 months or longer. Don’t try heroics.

4. Do not wipe the device(s), re-install software, remove software or allow antivirus to destroy anything. Set the anti-virus to Quarantine Only. The malware may need to be reverse engineered -- impossible to do if it is removed or destroyed.

5. Sequester the system. Remove it from the immediate threat, do not allow others (including I.T.) to use, touch, examine, or turn it off.

6. Use a write-blocker first, if I.T. must examine the device(s).

7. Save all logs. Make sure they are not being overwritten and take steps to authenticate the logs. Intercede the overwriting/destruction of log files.

8. Identify and collect any and all back-ups and stop the destruction/overwriting of the current backups.

9. Start with the End In Mind. After the event and things have settled, remember you’ll need the answers to these questions:
   • How did it occur?
   • What is the extent of the breach?
   • Do we have any notification duties?

   If the steps you take prohibit these from being answered, it could be worse than a breach itself.