Suffer a Data Breach? Here's Your First 24-Hour Checklist

Acting quickly and strategically following a data breach can help you regain your security, preserve evidence and protect your brand. According to Experian, it's important to collect, document and record as much information about the data breach and your response efforts, including conversations with law enforcement and legal counsel, as you can.

Once a breach is discovered, contact legal counsel for guidance on initiating these 10 steps:

1. Record the date and time when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.

2. Alert and activate everyone on the response team, including external resources, to begin executing your preparedness plan.

3. Secure the premises around the area where the data breach occurred to help preserve evidence.

4. Stop additional data loss. Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives.

5. Document everything known thus far about the breach: Who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected, what devices are missing, etc.

6. Interview those involved in discovering the breach and anyone else who may know about it. Document your investigation.

7. Review protocols regarding disseminating information about the breach for everyone involved in this early stage.

8. Assess priorities and risks based on what you know about the breach.

9. Bring in your forensics firm to begin an in-depth investigation.

10. Notify law enforcement, if needed, after consulting with legal counsel and upper management.

For more information on policies and procedures to protect non-public personal information, review ALTA's Title Insurance and Settlement Best Practices at www.alta.org/bestpractices.