HUSCH BLACKWELL

DATA PRIVACY

THE FIRST 24 HOURS

CHECKLIST

- ☐ **Contain the breach** by securing the premises around the area where the data breach occurred to help preserve evidence. Isolate and preserve compromised systems and data.
- ☐ **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.
- ☐ **Fix the issue that caused the breach.** Prevent further exposure of personally identifying information. Determine if you have other security gaps or risks.
- ☐ **Begin to execute your data breach response plan.** Alert the response team, including external resources, to begin executing your preparedness plan.
- ☐ **Engage your internal and external legal counsel and privacy/compliance teams.** Identify legal obligations including notification timeframes and requirements.
- ☐ **Record all information relevant to the breach.** All available data related to the breach should be collected at the direction of counsel so that the information can be analyzed to determine necessary remediation steps and legal responsibilities.
- ☐ **Determine the facts and circumstances of the data breach.** Interview those involved in discovering the breach and anyone else who may know about it. 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. Document your investigation at the direction of counsel.
- ☐ **Notify law enforcement,** if needed, after consulting with legal counsel and upper management.
- ☐ **Determine your approach to crisis management.** Engage your PR/crisis management team. Contain leaks about the breach.
- ☐ **Identify the key business stakeholders in addressing the data breach.** Include management, legal, IT, HR and external consultants.
- ☐ **Bring in your forensics firm to investigate the breach.** Secure compromised devices and preserve evidence. Analyze preserved and reconstructed data sources. Ascertain the number of suspected people affected and type of information compromised.
- ☐ **Identify critical business objectives.** Know what objectives might compete with addressing the breach.