Cybersecurity Incident Response Checklist

V&E

- ❑ Contact outside counsel to put activities under scope of attorney-client privilege
- ❑ Initiate incident response plan, including call tree
- ❑ Determine breadth, origin and nature of incident and whether it is an actual breach
- ❑ Determine the type and scope of data compromised, as well as the devices and systems affected
- ❑ Review cybersecurity insurance policies and notify carrier
- ❑ Don't reimage or delete files; preserve all evidence
- ❑ Order a litigation hold, if prudent
- ❑ Contact law enforcement, if appropriate
- ❑ Perform analysis of state, federal and foreign breach notification requirements for every data type compromised
- ❑ Develop uniform message for communications, including an appropriate description of the breach and compromised data
- ❑ Notify state, federal, or foreign entities as required
- ❑ Notify affected users as required
- ❑ Prepare for defense of third-party claims and governmental investigations
- ❑ Review and revise internal policies as necessary to document lessons learned