Cyber Incident Response Checklist

"Firms must adopt written policies to protect their clients' private information . . . they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."

– S.E.C. v. R.T. Jones Capital Equities Mgt.

- Determine whether incident justifies escalation
- Begin documentation of decisions and actions
- Begin mitigation of compromise
- Engage experienced legal counsel to guide through process, determine privilege vs disclosure tracks
- Activate Incident Response Plan and notify and convene Incident Response Team
- Notify cyber insurance carrier
- Notify affected business partners per contractual obligations
- Engage forensics to mitigate continued harm, gather evidence, and investigate
- Assess scope and nature of data compromised
- Preliminarily determine legal obligations based on type of data and jurisdictions
- Determine whether to notify law enforcement
- Begin preparing public relations message
- Engage notification / credit services vendor
- Investigate whether data has been "breached"
- Determine when notification "clock" started
- Remediate and protect against future breaches
- Confirm notification / remediation obligations
- Determine proper remediation services
- Assemble contact information for notifications
- Prepare notification letters, frequently asked questions, and call centers
- Plan and time notification "drop"
- Implement public relations strategy
- Administrative reporting (AGs, HHS, FTC, SEC)
- Implement Cyber Risk Management Program