

What to Do After a Cyber Breach

A Post-Breach Checklist for Corporate Counsel

- ☐ Escalate to outside counsel and establish a privileged communication channel; retain forensics and IR vendors to investigate quickly.
- ☐ Preserve evidence immediately; contain and isolate affected assets while balancing operational continuity.
- ☐ Start a data-impact triage by identifying what systems, what data, whose data, and where stored to inform regulatory analysis.
- ☐ Trigger cyber-insurance notice; confirm panel vendors and any consent requirements to avoid coverage issues.
- ☐ Map notification triggers and clocks across applicable regimes (e.g., HIPAA/HITECH, SEC cybersecurity disclosure rules, FTC Safeguards Rule, GDPR) and contracts; align public and customer communications accordingly.