PRIVILEGED AND CONFIDENTIAL
SUBJECT TO ATTORNEY-CLIENT PRIVILEGE

TO: [Recipient Name/Board of Directors]
FROM: [Legal Counsel Name]
DATE: [Insert Date]
RE: Legal Advisory: Cyber Extortion Risks and Incident Response

Dear [Recipient Name],

This memorandum outlines the legal risks and regulatory obligations associated with cyber extortion and ransomware threats facing [Company Name].

1. Regulatory Compliance and Sanctions

The payment of a ransom may implicate international sanctions laws. Specifically, the Office of Foreign Assets Control (OFAC) prohibits transactions with individuals or entities on the Specially Designated Nationals (SDN) list. Facilitating a payment to a sanctioned actor can result in strict liability civil penalties, regardless of whether the company knew the recipient was sanctioned.

2. Data Breach Notification Obligations

Cyber extortion often involves "double extortion," where sensitive data is exfiltrated before encryption. Under [State/Federal/International] laws, such as the GDPR or CCPA, the unauthorized access of personal information may trigger mandatory notification requirements to regulators and affected individuals within specific timeframes (e.g., 72 hours).

3. Fiduciary Duties and Governance

The Board of Directors has a fiduciary duty to oversee risk management. Failure to implement adequate cybersecurity controls or a formal incident response plan may expose the leadership to derivative lawsuits for breach of the duty of care.

4. Evidentiary and Law Enforcement Engagement

To mitigate legal exposure, it is advised that:

- All communications with threat actors be handled by specialized third-party negotiators under the direction of legal counsel.
- Law enforcement (e.g., FBI/CISA) be notified promptly to establish a record of cooperation.
- A forensic chain of custody be maintained for all digital evidence.

5. Recommendations

We recommend an immediate review of the company's Cyber Insurance Policy to confirm coverage limits for "Cyber Extortion" and "Business Interruption." Furthermore, the company should update its Incident Response Plan (IRP) to include a specific protocol for ransom negotiation and payment authorization.

Please contact us to schedule a formal briefing on these matters.

Sincerely,

[Signature]
[Name of Legal Counsel]
[Law Firm/Department Name]