The Comprehensive Checklist for Cyber Insurance

1. Assess Your Cyber Risk Profile

- [ ] Evaluate the types of data collected, stored, and processed (PII, financial records, intellectual property, health data).
- [ ] Identify applicable data protection and privacy regulations (GDPR, HIPAA, PCI DSS).
- [ ] Analyze operational dependencies on digital systems, third-party vendors, and supply chains.
- [ ] Complete a formal cyber risk assessment, including scoring critical assets, vulnerabilities, and threat exposure.

2. Quantify Potential Financial Impacts

- [ ] Calculate expenses for forensic investigations, data recovery, customer notification, credit monitoring, and legal fees.
- [ ] Estimate potential revenue losses from business interruption caused by system downtime.
- [ ] Assess potential ransom payments and costs associated with ransomware recovery.
- [ ] Evaluate reputational damage and costs related to customer attrition and increased marketing efforts.
- [ ] Identify indirect costs such as reduced stock prices, regulatory audits, and increased insurance premiums.

3. Evaluate Coverage Needs

- [ ] Confirm first-party coverage for direct losses (data restoration, business interruption, cyber extortion, incident response).
- [ ] Verify third-party coverage for external claims (legal defense, settlements, regulatory fines).
- [ ] Ensure access to a network of experts for incident response (forensic investigators, legal counsel, cybersecurity specialists).
- [ ] Review the need for industry-specific riders addressing regulatory fines or liabilities (e.g., healthcare, finance).

4. Scrutinize Policy Terms and Conditions

- [ ] Identify coverage triggers (data breaches, network security failures, cyber extortion).
- [ ] Understand policy exclusions (acts of war, insider threats, outdated software).
- [ ] Check for retroactive coverage for incidents occurring before policy inception but discovered later.
- [ ] Ensure coverage applies across all regions where the organization operates or serves customers.
- [ ] Review sub-limits applied to ransomware payments or regulatory fines.

5. Assess Insurer Expertise and Support Services

- [ ] Select insurers with proven experience in cyber insurance and emerging threat understanding.
- [ ] Look for proactive risk management services (training, threat intelligence, vulnerability assessments).
- [ ] Evaluate the insurer's claims handling performance (response times, approval rates, client satisfaction).

- [ ] Confirm insurers offer real-time threat intelligence and ongoing risk scoring during the policy period.

6. Implement Robust Cybersecurity Measures

- [ ] Conduct regular employee cybersecurity awareness training.
- [ ] Enforce strong access controls (multi-factor authentication, least privilege principle).
- [ ] Ensure timely software updates and effective patch management.
- [ ] Apply encryption for sensitive data (in transit and at rest).
- [ ] Maintain and update a comprehensive incident response plan.
- [ ] Run regular tabletop exercises simulating ransomware and insider threat incidents.

7. Strengthen Legal and Compliance Measures

- [ ] Ensure compliance with relevant data protection laws and regulations.
- [ ] Review contracts with clients, vendors, and partners to identify cyber liability obligations.
- [ ] Understand breach notification requirements applicable in relevant jurisdictions.

8. Continuously Monitor and Update Coverage

- [ ] Review your cyber insurance policy annually to align with evolving risks.
- [ ] Adjust coverage limits based on business changes and risk landscape shifts.
- [ ] Explore new policy offerings and enhancements available from insurers.