Cybersecurity Checklist:
8 Questions To Ask You Current Security Provider

1. What is your philosophy or approach to cybersecurity? Should we have a cybersecurity plan or roadmap?

2. How often should we be meeting to discuss cybersecurity? What are the critical topics we should be discussing?

3. What Cybersecurity services and tools are provided through our contract? Why this collection of tools and services? Are they sufficient to protect my network/data as well as to detect possible threats?

4. For each of those services and tools, how should I regularly measure whether they are implemented successfully and performing their intended function?

5. What best practices are your other clients implementing that we are not currently? Some examples would be policies around the use of personal devices and the implementation of a corporate-owned password manager.

6. How should we think about the division of responsibility/accountability for cybersecurity? What responsibilities do you have for the security of my network? What responsibilities do I, my staff, or other service providers have?

7. Have you provided my organization with a Cybersecurity Risk Assessment based on an established framework (such as the NIST Cybersecurity Framework or ISO 27001)? Is that a service that you offer or recommend?

8. Have you helped my organization develop an Incident Response Plan in the event of a Cybersecurity incident (email compromise, ransomware, data breach, etc.)? Following a cybersecurity incident, what services would you provide vs. what I need to implement myself?

Don’t be the next company name under the data breach headline; consult one of our cybersecurity experts today.