Cybersecurity RFP Considerations

Cybersecurity means a lot of things to a lot of different people. Cybersecurity includes technical solutions for security (such as anti-virus software), internal organizational processes and procedures (such as requiring passwords to be changed every 90 days or training your staff on cybersecurity awareness) and externally facing solutions (such as vulnerability scans). Each one of these items requires separate solutions to ensure the highest level of security.

Put another way, there is no “one and done” or “set it and forget it” solution for cybersecurity. Organizations need to approach cybersecurity from a strategic, holistic perspective. When crafting your RFP, it’s also important to be cognizant of the fact that organizations operate in a continuum of cybersecurity maturity.

From a 50,000-foot level, a cybersecurity RFP should share a baseline of your organization’s current capabilities are (where are you now) and what your organization’s needs are (where do you want to be). Respondents should lay out the pathway on how you they envision fulfilling this request (how do you get there).

If you are at the beginning of your cybersecurity journey, we suggest looking into existing cybersecurity frameworks, such as the NIST Cybersecurity Framework (CSF), or a prescriptive standard like the Cybersecurity Maturity Model Certification (CMMC) or PCI. These frameworks and standards are not exactly light reading, but there are several existing self-assessment tools that can help you establish your own baseline.

If your objective is to become compliant with a particular framework or standard, the first step in your RFP process may be to engage with an MSP or MSSP to perform a gap analysis. A gap analysis will analyze your current cybersecurity posture against one or several frameworks or standards, inform you of where your current practices meet the standard, and then provide you with an actionable remediation plan. That remediation plan can then be used as the basis for a future RFP.

Either way, it’s also essential to provide the following important details to assist a vendor with scoping:

- How many users, workstations, servers, applications, physical locations, data center locations, public cloud providers, and SaaS providers do you need to provide a cybersecurity solution for?

- Clarify if you’re looking purchase specific tools, looking for a vendor to implement or optimize tools you already have, or seeking a vendor who can look at your environment strategically and make recommendations aligned to a particular standard or framework?

- If you need vulnerability scanning (or think you might need it), how many external (Internet) facing IP addresses do you have?

- If you may need penetration testing, how many distinct web sites / web applications are in scope?

Having been the one responding to many IT infrastructure and cybersecurity related RFPs, we also strongly advise the following:

- Provide a mechanism to allow respondents to interact with your project team prior to submitting a final RFP. Ideally a pre-bid webinar that involves your SMEs.

- If you’re going to provide a Q&A period, allow yourself sufficient time to distribute the questions and collate the answers.