Have you appropriately identified and defined (documented) your IT system boundaries for CMMC compliance?

As organizations work on preparing for eventual CMMC certification, one of the critical factors that must be addressed at the beginning of the process is what your scope or boundary will be. This is not a one-size fits all process, and Organizations have a lot of choices that can impact costs and overall organization IT risk.

Here are a few of the key things we consider when helping organizations define their CMMC boundary.

1. **Where is the data?** - Your CMMC boundary must first and foremost follow the data. If you process CUI and/or FCI, you need to identify **ALL** locations where you collect, process, store, and transmit this data.
   a. Start with your DoD contracts and determine where that data is located. Do not forget to look at older contracts where you may still have data.
   b. Have discussions with individuals on those contracts to determine how they are handling the data.
   c. Talk with IT and determine if data is moved offsite for storage or redundancy. Where do they think the data is located?
   d. Note where data your organization has been entrusted with is being managed, processed, or stored by third-party organizations outside of your direct control. You are still responsible for that data.
   e. At the end of this exercise have an inventory of sensitive data that at a minimum identifies what CUI / FCI is handled and where it is located. Consider including other types of sensitive data (PII, PHI, etc.) in this inventory if possible. It is a corner piece to good cybersecurity and risk management.

2. **Is the current process appropriate?** - Once you understand where the CUI / FCI is, you can determine if that is appropriate. Many organizations realize they have sensitive data (CUI / FCI) flowing through or sitting on more portions of their IT infrastructure than they knew or would prefer. CUI is often residing on employee laptops, sitting in email, or sitting in random folder across the network. Without strong data handling policies, users often create copies of the data that wind up in different locations. As you define your CMMC boundary, you should try and minimize the locations where this data will reside.

3. **To Segment or Not?** – For many organizations, a key question they have is whether to apply the controls, policies, and procedures required by CMMC (level 3 and above primarily) to the entire organization or just a portion where CUI / FCI resides. So long as you are covering the CUI / FCI,

For more information, on how we can help you with your CMMC compliance or Risk Management efforts please contact us at gbills@logicalsecurityservices.com.

there is no perfect answer. Some of things to consider when deciding how much of your organization to include in the scope should include:

a. **How large is my organization?** For large organizations, their government practice might already be a separate segment or line of business. Key things that would help determine this include whether the government practice has their own network, systems, or IT processes. In these cases, carving out the government or even DoD practice might make sense. For smaller organizations, where they don't have separate lines of business and the IT infrastructure is shared by all, segmenting out a piece for CMMC probably does not make the most sense.

b. **How many contracts do you have where you handle CUI or FCI?** If your DoD work is a small portion of your business, it might make sense to try and isolate that data to a small portion of your network. There are several products on the market that offer encrypted storage of data. These products in conjunction with strong data handling policy and procedures may be the most cost effective and efficient choice.

c. **Do I want separate controls, policies, and procedures for different portions of my organization?** As a rule, the more complex your organization is, the more risk you are probably introducing. From my 20 years of auditing organization, I have seen that having different controls, policies, and procedures for different parts of your organization increases the likelihood of those processes not being carried out consistently. Usually, the more you can have one process followed by everyone, the more likely that process will be consistently and effectively carried out.

4. **Third-Party Providers –** Make sure to clearly identify what third-party service providers have access to your CUI / FCI. Access is the key focus here. It can mean they have your CUI / FCI on their systems or they have access to your CUI / FCI on your systems. Clearly identify who the third parties are and what type of access they have. You should also have detailed contracts in place that clearly identify each parties' roles and responsibilities for safeguarding CUI / FCI.

5. **Document, Document, Document** - Document your boundary as clearly as possible. Also maintain documentation of how you identified your boundary. Your CMMC boundary should be one of the first things the C3PAO auditors focus on to understand what their scope is. Be prepared to answer questions about how you came up with this boundary and how you gained comfort that CUI / FCI is not being collected, processed, or stored outside of this boundary.

For more information, on how we can help you with your CMMC compliance or Risk Management efforts please contact us at gbills@logicalsecurityservices.com.