Transcript – What Google Can't Tell you about NIST 800-171 Compliance – Part 2

00:00:00 Introduction

Welcome to Cybersecurity Magnified with Braxton Grant Technologies, where candid cybersecurity conversation needs technical and applicable advice. Investigate with our experts on the latest in the cyber world, including security best practices, compliance guidance, and all things cloud adoption. Thanks for joining the conversation! Let's get started.

00:00:31 Krista, Podcast Host

Hello everyone, and welcome back to Cybersecurity Magnified. Once again, I'm Krista and I'm joined by Josh, one of our cyber security engineers. This is part two of our NIST 800-171 compliance series and we're going to be building off the previous episode, so if you haven't listened to that, check that out.

First, we go over a lot of key concepts you might find helpful as we dive a little bit deeper into this episode. And don't forget to subscribe to Cybersecurity Magnified to stay up to date with all upcoming episodes. We're available on Spotify, Anchor, Google Podcasts, and Breaker and all episodes are also available on our website, which is braxtongrant.com.

To recap, at the end of last episode we had started talking about documentation and policies and procedures relating to NIST 800-171.

00:01:23 Josh

Yeah, so we mentioned quite a bit about the documentation and how important that is to CMMC and also to NIST. And the initial information that we're getting out of the pilot contracts that are being certified for CMMC is that documentation, policies, and procedures are a big part of what's missing for a lot of companies, and they're putting emphasis on that. That's an area where companies really need to focus in on to ensure that you have all these documented policies and procedures so that it sets the tone for the company's maturity level and their cybersecurity as a whole. Having all these things defined in writing and agreed upon by the company and setting the expectation for the employees. So it's not surprising that there's a lot of focus on these core business operations, and that documentation tends to be an afterthought for a lot of companies. Writing out procedures or standard operating procedures, those kinds of things, are one of the first things to get done and they usually are the last things to get done, so CMMC is putting a lot of emphasis on that. When you read through the controls, they're expecting to have plans, policies, procedures, and documentation that shows how things are done, especially in relation to the domains and the practices within CMMC.

00:02:48 Krista

And what does this look like when an organization is starting this process?

00:02:54 Speaker 3

So when you look at policies and procedures and documentation, there's sort of a flow down, like a hierarchy, that kind of dictates the order that these things kind of flow. So at a high level at the top, you

looking at your policies, you know those are your expectations from the company to the employees- or expectation from management- to how the company should operate or how they should accomplish certain things. It's a high-level document with the expectations in it doesn't dive into the exact details, but at least sets the expectation of how things are done within the company and what the expectation is.

And then from there, you have your standards that help dictate the procedures on how these things are actually accomplished. Your procedures are one of the next important levels to dictate how the policies- what's stated in the policies- are actually accomplished on a day-to-day level. You know, those procedures of the individual things that are done help show the employees how it should be done and in that process. You're dictating not only what the expectation is, but how it should be done.

And below that would be guidelines. Maybe things that are not set in stone, but that should be followed or should be considered as these different procedures and things are accomplished.

00:04:16 Krista

Yeah, and I think another thing that if to keep in mind is if you have a person that understands writing this documentation internally.

00:04:24 Josh

Yeah, for sure. You know, it definitely requires a certain sort of skill set and time, energy, and resources to actually be able to sit down and write these sort of things. And this is a good place where maybe a company can bring in an outside consultant to help with this kind of writing and stuff. There's a lot to cover in NIST and CMMC as far as policies and procedures. Policies are one of the bigger areas that an outside consultant can really provide a benefit.

And you know, getting that outside help can really get a head start, and get that high level initial documents done, or at least drafted up. It might need some polishing up or some tweaking, but once that parts are done then everything else will, you know, help to fall into place. And then it becomes a matter of writing out standard operating procedures for different work and actions that fall under the domains of CMMC and NIST.

00:05:27 Krista

Yeah, and even if an organization is able to start and then an outside consultant can fill in the gaps, you can kind of fit what's best for your organization, right?

00:05:43 Josh

Yeah, absolutely. You know, it depends on the organization. It depends on what's already done and what needs to be done. You know, the company may already have some policies. Maybe there are numbers that you know already covered distance CMMC domains. Maybe there's a lot missing. It depends on each individual company and how much work needs to be done in that area. And so that's just something that has to be weighted by the company management – how much work needs to be done to be NIST and CMMC compliant. And you know, if there's a very large amount of work that has to be done, then it makes sense to try to get as much done by bringing in outside help. And then you can focus on the areas where things can be done internally.

Also in regards to bringing in outside help- what can be done internally and what can be done externally by a third party- is a lot of companies procure services through MSP and other service providers. So something that companies can take into account is to not only determine what they're doing themselves internally, but if you have service providers that do procedures or cover things that are within the domains and practices of CMMC and NIST, then you need to understand who's responsible for what. In regards to like an MSP- are they responsible for the antivirus? Are they responsible for patch management? At the end of the day, it's your company's compliance that has to be proven. So if you have an outside provider, you need to make sure that you understand what they're responsible for, they understand what they're responsible for, and that can be communicated back and forth. And when it comes time to actually do an assessment and prove compliance, that they can provide the correct amount of evidence to show what they are doing, and also that they have the procedures, that they have the security around what they do that involves your assets and your data.

00:07:41 Krista

And any other advice in regards to documentation, policies, procedures, etc.?

00:07:49 Josh

Yeah, I think one of the biggest things that a company needs to keep in mind, especially if they don't have a lot of policies and procedures yet, is that if they're going to go and start to draft up these policies and procedures, or even if they're going to have it their party do it, is to ensure that they're realistic to the company. That there actually is something that they can accomplish themselves. There's a lot of templates and there's a lot of examples out there for policies and things, but companies need to read through it and see what it actually states. There's no point in writing up a policy that says all these things if you know at the end of day they're not actually going to be followed by the company. So there's a company culture aspect to this that needs to be considered as well so you don't just write up a bunch of expectations that, realistically, the company or the employees are never actually going to follow. So, I would say that think about the company itself and what the company culture is. There's probably going to need to be some new things that are added that you're not doing yet, but don't expect that if you just write a policy that it's just magically going to be followed.

And also, I think you know in regards to that too, a company needs to understand that if they're going to write all these new policies and procedures, that then needs to get disseminated to all the employees and that everyone understands what it is that needs to be done. There's a whole culture shift that now needs to happen to bring everyone into compliance and understand that how and what they're doing is important to whether the company is NIST and CMMC compliant.

So, drafting up procedures is great. The next step after that is to make sure they get approved by the appropriate people, they get disseminated to the employees, and everyone understands what they're reading and understand what needs to be done, and that's a big aspect to it as well. Because at the end of the day the company needs to live and breathe this. The documentation isn't just there to prove compliance once every three years and then walk away and never look at them again. It should be the documents that the company is operating off of on a daily basis. You know, not just the procedures, but also the policies that should be all the day-to-day stuff of how the company actually operates and what the expectations are. So that's an important thing to consider, and that you know writing all this stuff, make sure you write it to be realistic to what the company can actually accomplish.

00:10:16 Krista

Yeah, and that kind of goes back to our last episode and we kind of covered a more high-level overview. You had really drilled in in that episode about, really, it takes everyone and takes different departments and other things like that as well.

00:10:31 Josh

Absolutely yeah, you know, it involves everyone in the company. It involves all different aspects that the company operates on the day-to-day basis. So yeah, it's important that this kind of filters down, and as I mentioned, it's a culture thing. You know it should be a company culture thing. And that's part of whtit's called the Cybersecurity Maturity Model.

You know, they're talking about maturity, and if a company or an organization has a mature cybersecurity program, it's because all this information and all these expectations are, you know, baked into the company culture and disseminated down to all the employees. And everyone understands what they need to do and to ensure the company is secure.

00:11:10 Krista

With that being said, stay tuned for our next episode in the series on maximizing investment in technology to become compliant. Josh, thanks so much again for joining. And we'll see you next time.

00:11:23 Outro

Thank you for listening to Cybersecurity Magnified. Make sure to subscribe wherever you get your podcasts, so you're up to date with our newest episodes. And if you found this episode helpful, share it on social media. Braxton-Grant is an experienced cybersecurity solution provider with over 20 years of experience in the government and commercial space. To learn more about us, visit braxtongrant.com or find us on LinkedIn. Thanks again for listening!