Transcript- What Google Can’t Tell you about NIST 800-171 Compliance- Part 3

00:00:00 Intro

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. I'm Krista, and Josh is back with us continuing our NIST 800-171 compliance series. If you haven't seen the first two in the series, be sure to check those out. Our first episode we go some key concepts and recommendations for getting started, and part 2 we dive into specifics of documentation and how important that is for your compliance journey.

Both of those episodes are available now on Spotify, Anchor, Breaker, or Google Podcasts, as well as our website which is braxtongrant.com. And don't forget to subscribe so you don't miss out on any upcoming episodes.

Today's episode is all about maximizing your investment in the technology to become NIST 800-171 compliant. It’s no secret that the importance of putting time, money, and resources to this problem is really important, but obviously once you have your plan developed, you want it to work as efficiently as possible.

So, from our previous conversation, it seems like there's a lot of groundwork that needs to be covered to become compliant, and technology plays a huge role in this. So where should companies start in deciding what types of technology to use?

00:01:49 Josh

Every organization has different needs and requirements, and there's no one size fits all technology out there that’s going to be the best solution for every company. Small companies can be different than a large team, and that’s going to be different than a medium company. How companies operate and what their layout is and their processes are has a big impact on what technologies they need, what they use, and then what tools and systems on top of that can be used to gain compliance if need be. So, you know, the companies need to take a look at how they have implemented their technology, and what kind of options are out there.

And one of the biggest differentiators right now is the subscription-based model versus the more traditional model off the shelf: buy a product and set it up within your own internal network. And there’s pros and cons to both of those, and what is a “pro” to one company is different than another company. It depends on their size and whatnot. We find that companies on the smaller side can do really well with subscription-based products and tools because it’s a very low cost to get it initially. You just pay by the month. It’s very scalable. You pay by just what you need. Most of its generally just based on user licensing- how many people do you have that need it- which makes it a very easy investment to get into.

Larger companies may have more infrastructure and more personnel to build their own tools and systems internally that they buy. Generally, if you're going to buy a software or technology or product that has to run off of the server, well, then you got to build the server and you have to have a cluster of servers to run all that and how they interact. Then your network all has to be managed internally and whatnot, so that increases the complexity of some of these solutions. When companies look at what's out there, they need to understand what the cost is- is it a big upfront cost? Is it a low monthly cost? Is it something that can be paid off right away or that you're going to end up paying for the life of your subscription? How does that impact your budgeting? And then also the complexity and how it's used and how it's built, how it runs. So you know, like I said, it's no one size fits all for a company.

These, I think, to start companies really need to understand what is the problem that needs to be solved. You don't want to get into buying technologies just because they sound great or because they're flashy or the sales pitches and all that stuff. You want to understand what's the problem? How is this technology going to solve that problem? And determining how the technology can solve the problem can help you determine what's the best bank for your buck. What increases compliance gain, reduces risk, improves efficiency, increases productivity. All these things will help companies make the right decisions in purchasing technologies to solve these problems.

00:04:47 Krista

Yeah, it just sounds like setting any other goal in a business that you want to accomplish of then kind of working backwards from that end goal and finding what works best for you and for your organization and that sort of thing.

00:05:01 Josh

Yeah, exactly.

00:05:04 Krista

And if I'm a business owner and trying to fix a specific problem, how is the best way to search and discover the right technology that will not only serve my needs, but also be within my budget?

00:05:17 Josh

So this is a great opportunity for, you know, a company to bring in a trusted partner or consultant to help with these technology purchasing decisions. We've seen a number of companies that, once they realize how much needs to be done to be complaint with NIST and CMMC, that understanding that bringing in outside help can really significantly assist a company with making progress and gaining compliance and whatnot.

Companies sometimes might make the mistake of, well, we'll just do this internally because we don't want to have to spend too much money, or we have some people that maybe can handle it. But you got to realize that people that are already working within the company already have their roles and responsibilities, can they take on additional decision-making, research, and understanding what technologies are and really being fluent in them to make the best decision.

Oh, so you know, there's several different ways a company can do that. Then there's got plenty of you know Managed Service Providers out there and Managed Security Service Providers that can really augment your staff internally to provide either tools, purchasing decisions, or services that will help you gain compliance. And doing those can actually help a company really gain compliance much more rapidly and help them provide the policies, procedures, and technologies through a third party, so that they don't actually have to then build and maintain all themselves. Having a resource that really understands the different technologies and has an understanding of your business process is really important because you know to make the best decisions on which technologies and which services to utilize, you really have to understand how your company operates. And if someone else, a third party or an outside consultant, is going to help with that, they need to understand how your company operates and how this technology is going to impact and benefit your company. So that really can be a key point there.

And also understanding your organizations IT infrastructure. Are you in the cloud? Are you on-premise? Are you both? Are you using a lot of SaaS-based applications or using cloud-based infrastructure? How do all these different pieces fit together and how does this impact your company's compliance? You really need to understand that. And if you're not fluent enough in all these different technologies and what you're actually utilizing and how it impacts, then you really do need a third party or a consultant to really explain it to you and walk you through it so that you can make the best decision possible.

00:07:58 Krista

So, if a company uses a service provider to manage its technology, how does that impact compliance for NIST or CMMC?

00:08:07 Speaker 3

So, when you bring in an outside service provider. Generally, they're providing some sort of service that will help you gain compliance or provide the procedures and the actual day-to-day operations that satisfy that control, whatever that may be, or multiple controls. So your company really needs to have a good communication channel with the service provider and agreements on who is responsible for what. At the end of the day, it's your compliance, so if there's a service provider that's providing some sort of service to you that impacts your compliance, they need to understand how that's important to your company, and they need to be able to apply the appropriate policies, procedures, and evidence and whatnot to ensure that when you go into an assessment, that they are there to help you prove your compliance and ensure that they're doing it properly as well.

Also, you know whatever technology solutions they're using, they need to understand whether those are satisfying NIST requirements or CMMC requirements as well. So choosing a service provider that's well versed in CMMC and NIST compliance is really going to help a company ensure that when they go to actually do an assessment, that those outside service providers can provide all the information that's needed to prove the compliance.

And also again, those service providers need to have policies and procedures for the standard operating stuff, the day-to-day operations that affect your compliance. If you have a Managed Service Provider that is managing your endpoint protection and managing your firewalls, and you had internal access to your networks and has admin accounts and has the ability to change configurations and stuff, then all that has to be documented. All that it has to be within their policies and procedures because they are the ones doing it. And all that has to be NIST and CMMC compliant because you are essentially offshoring that or outsourcing those operations, which are covered under NIST and CMMC, and therefore, it is still your compliance that is affected if they're not doing it properly.

00:10:24 Krista

And for those companies that have more of an internal IT team, how would this advice be different?

00:10:32 Josh

So you know a lot of the same kind of gotchas apply as to ensuring policies, procedures, documentation on how the organization is compliant. It still applies, it is just now these operations are managed internally, so you need to ensure you are managing all the policies, procedures, how the team is managed, what it is they're doing, and make sure that is compliant, versus having an outside provider that you're paying now, but they're responsible for certain actions and having that agreement with them. Pretty much every organization has numerous service providers, regardless of how big their IT team is or how big their IT department is. They work with those service providers to have different services- that may be cloud-based services, offsite storage locations, data centers, that kind of stuff. So its really important for the IT team or the company to understand who is still responsible for what. You know, regardless of whether you're using software-as-a-service infrastructure, servers platform as a service or other services like this, you know it's important to understand where the responsibility lies. You know the internal team may be responsible for a lot of the configuration of how you know how the company uses those services. But at the end of the day, there is still a whole other element of that infrastructure that the service operates on, that someone still responsible for. And when you look at SaaS-based applications, infrastructure services, platform as a service, there's varying degrees of responsibility of who's managing what. When you talk about software, the service really, you're talking about your company or your team is probably managing the configuration of the software settings, but that still runs off of some data center somewhere of servers and networking and all this stuff that you don't necessarily have to manage, but somebody is. How is that potentially impacting your compliance? You can't just stick your head in the sand and be like, well it's not our problem. We don't touch it. Somebody does, so somebody needs to be responsible for it, and understanding how that impacts your compliance is pretty important.

You know, having your own internal team all is well. Again, make sure you have all the standard operating procedures, policies, documents and understand how your team is meeting that compliance. And it can still be worthwhile to bring in outside help to assist with numerous different aspects, whether that's, you know, implementing new technology, doing proof of concepts you know for something new that you want to implement, demos, helping make recommendations, Again, if you have an internal team, they're working on their day-to-day workflows and responsibilities, so they may not have the time and the resources to figure out what's the best solution or know what's out there and how that can best solve problems for your organization.

00:13:34 Krista

And then really just pulling it all together, how does a company know whether their investment in technology is paying off?

00:13:42 Josh

Yeah, so it's always important for an organization to understand if you've now purchased, implemented, or deployed, that a technology or solution is having the desired effect. Some things are very easy to tell, some things not so much, and you got to make sure you cover the bases and understand once something’s been, once a project has been completed, is it providing the services and the benefits and meeting the requirements that you thought it was?

This really is a matter of somebody going back in a lot of cases and checking. Who is going to go check and ensure that the desired effect is being accomplished, that was configured properly that its been deployed and it is actually working on every single system and endpoint that you thought it was going to be on and is it effective?

And understanding in most cases tools or technologies don't automatically satisfy NIST and CMMC compliance by themselves necessarily, you still have to have documentation, diagrams, architectural designs, policies and procedures. All these other things that go into proving your compliance. And really painting the picture of how do these elements and things that help you satisfy compliance satisfy the requirement? How do they actually do it? Because you have to prove it at the end of the day and you have all this backup information, and it’s not just a matter of just installing something and walking away.

And this could be ,again, another good source for an outside provider or a consultant that can come in and help you do a readiness review or a Gap Assessment to ensure that what you have in your technology arsenal and what you've deployed is actually meeting your requirements. And then on top of that, ensuring that what you have for evidence or policies or procedures is actually going to be enough when you actually need to walk into an assessment one day.

00:15:51 Krista

And getting a Gap Assessment from an organization like Braxton-Grant can be a great place to start, no matter where you are in the compliance process. We look at your existing information systems and security measures and we identify gaps in your CUI and cybersecurity protections.

So if you are interested in learning about our Gap Assessment, or if you're interested in other ways that we can partner with you as a consultant to these types of compliance standards, we would love to have a conversation with you to further understand your organization needs. Feel free to check out our website, braxtongrant.com, and there you can find a whole bunch of information on how we serve our customers. You can fill out an inquiry form or give us a call, whatever is easiest for you. Once again, that’s braxtongrant.com.

00:16:44 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!