Giesler Seaside Chats:

With Dan Berger and Steve Harris

of First Team Cyber

Patricia: Good afternoon and welcome to our Giesler Seaside Chat. I'm Patricia Giesler and we are woman veteran owned small business focused on providing I.T. services. Today, I would like to introduce you to Dan Berger and Steve Harris, who will educate us on the CMMC process. Dan, Steve, could you tell us a little bit about yourself and your experiences?

Dan: Thank you very much for allowing us this opportunity to share our experiences with you today. My name is Dan Berger and I have 25 to 30 years of IT experience. Over 20 of it is in the cybersecurity world, in the Department of Defense Industry and some other industries, such as health care and finance.

Steve: Again, thank you for the opportunity Patricia. My name is Steve Harris. I'm a retired senior naval information warfare officer with a 41 years of experience in the cyber security world. I've my most recent commands. I was director of Office of Compliance and Assessment for the Navy, conducting cyber assessments on ship and shore facilities throughout the world, and also then with Naval Network Warfare Command in San Diego, working with ship and shore facilities with their cybersecurity needs. And as well as working with First Team Cyber now for the past three years, conducting assessments and other things for industries throughout the United States.

Patricia: Okay. So I kind of have a great idea now of why you guys got into the cybersecurity field. Obviously, your Navy careers led you there. What do you think today is the biggest challenge that small businesses are facing in the cybersecurity realm?

Dan: What not to do? That's the biggest challenge. There's so much coming at the small business forces from resource restraints, like not having enough people. You know, the hiring problem, the financial problem with the economy, the bad actors are just growing exponentially. And we're seeing a lot of different sophisticated attacks coming through now. And it's really hard for them to really understand, you know, where to focus their efforts to secure that important information or that asset that they own.

Steve: Yeah, I agree with Dan. You know, if I could sum it up in a single word, it would be everything. Not only do these companies or people have to worry about threats from the outside, they certainly have to worry about the threats coming from inside their companies. So the attack vector that Dan mentioned is not only one of those things where you have to worry about certain aspects, you have to worry about all of them. And with all those challenges, all of the challenges that are out there right now and with lots of resources available as well.

Patricia: Could you give us any guidance or direction on a good location to be able to get accurate information that'll tell us kind of, you know, what is the current state, what do we need be in compliance with such as NIST 800 171?

Dan: It depends on many factors. It depends on what type of organization and what the regulatory requirements, you know, are hanging over their head. You know, if you're a health care organization, you have HIPAA. If your organization is that process, credit cards, you have PCI. If you're a Department

of Defense contractor, you have the FAR and DFAR regulations that require compliance to one of the NIST's models, SB 800 171, as you described. That is another challenge. Where do you find those resources? There is a very valuable resource that the federal government has stood up that you can subscribe to that will give you the most formal exploits are out there. And then they also have additional resources that you can tap into. But finding a good consultant that you trust that specializes in cybersecurity would probably be your best resource because they have all the tools and they're plugged into all the different regulatory bodies and everything, you know. So you're bringing in a trusted single source as opposed to trying to digest all that information find that you want.

Steve: They can also visit the NIST website, which is certainly easy to get to. It's www.nist.gov. All of the necessary publications and guidance certainly can be gotten there gleaned from that website.

Patricia: Yeah and I know you guys right. So I trust you. I at least have a good advantage there. So Cybersecurity Maturity Model Certification 2.0 program is designed to reinforce information security requirements for the Defense Industrial base. What do small businesses need to do to prepare for the full CMMC rollout?

Dan: Steve and I are the co-founders of First Team Cyber. We were founded on the basis of helping Department of Defense, small and mid-sized contractors meet the current regulation that requires them to be compliant. It's a regulation that's been around for several years. It's nothing new and it if you go into your Department of Defense contracts and you see a clause that's a FAR 52.204 21, which is basic safeguarding of covered contract information. If you have that and or you have DFAR 252.204 7012 which covers the safeguarding of covered defense information and also brings in the cyber incident reporting requirement. Those clauses are in your contract. You must meet the NIST SP 800 171 compliance list of controls, which is a list of 110 controls for cybersecurity and it's all under this protecting the controlled unclassified information or we call it CUI or C-U-I. That is the current requirement. The federal government is looking at new regulation that is still being developed and it's about ready to go out for review and comment by the public. And once it goes through that process, then they have time to revamp that until it's actually signed into law and that is called CMMC. So right now, CMMC is a future state. It's not a current state. So I hope that sheds light on what their current requirements are. The current requirements are what's in the FAR and DFARs clauses that were in their contract. If they don't have that in their contract, there's no compliance requirement. But I'm 100% confident that any Department of Defense contractor or subcontractor out there has those two clauses in their contract or subcontract.

Patricia: So considering that CMMC is a future state, what can small businesses do now to focus on getting CMMC Level one compliant?

Dan: They should perform an assessment, they need to have a NIST SP 800 171 assessment completed. Now there's various ways you can do it. You can self-assess or you can have an organization like us come in and do it for you or a third party. That assessment has to be done. And then the results of that have to be registered in the SPRS database, which is the database that allows the contracting officer or federal government to validate that you're meeting that law so they can grant you, you know, the contract you won or they don't take it away from you. So the very first thing they need to do is they need to have an assessment and along with that, there needs to be a system security plan developed and published that basically is the parameters around what the assessment is, what you're assessing against.

Steve: And inside that system security plan is basically has the 110 controls, which is also your POAM, which is a requirement in SPRS as well.

Dan: Steve, elaborate a little bit on what a POAM is. Just for people who don't know that.

Steve: A POAM is a plan of action in milestone, with each control, you have four levels. It's either compliant, non-compliant or I think three sorry, compliant, non-compliant or in process. And compliance is the only way you're going to receive a positive score in process or non-compliant. Obviously, you're working on it, but inside the POAM you're going to be assigning a date and you're also going to be assigning a person or persons who is going to be working on that particular control to remediate it within a timeframe. Now, within that, you have six months in order to complete that. So if you have if you if you're non-compliant with all 110 controls, you have six months to get compliant with those or at least bring your score up to what would be considered a acceptable score to a contract manager to allow you to secure a contract or if, if you will, in this case, and a lot of times your prime who you may be sub down to make them feel like you've got control of the situation and you also are doing the right things on trying to get yourself to 110 points or 110 out of 110 controls.

Dan: There is a fourth category on that. If you decide that that control is not applicable, you have to produce documentation of why it's not doesn't apply and you're supposed to submit that to the federal government and get them to approve it. Otherwise they consider it applicable and you must meet it. And a lot of people don't understand that piece. You can't just say, Oh, it doesn't apply to me and just ignore it. It has to, you have to document it. So when the auditor comes in, he sees that it truly isn't part of your security program. And the federal government agrees.

Steve: And a good example of that would be like a VoIP phone. A lot of companies don't have a secure phone network and that would be one that would be a good example of a not applicable that it would have to be approved in order to mitigate that control.

Patricia: Can you tell me what your process is for helping small businesses get ready?

Dan: It all starts with sitting down and understanding their organization and understanding what information they actually are receiving, processing, producing, storing and or transmitting back outside the organization. And then classifying that information. In reality, is it truly CUI data or not? And once that is done, then we would develop the systems security plan for them and build those boundaries because we know where that information is. And then conduct an assessment. So under those steps, it's a risk analysis. It's a information flow and a development of the scope of the network that would fall under that regulation. And then once we do that, then we would assess to make sure that they have the 110 controls in place. Once that is complete at step one, we would move to a development of the POAM, which is part of a gap analysis. And then we would work with that organization to put a plan together to mitigate those controls so they can meet that regulatory body. And we understand a lot of organizations, especially small ones, may not have the resources or the funding. So we work with them to help prioritize what to remediate first. Nine times out of ten, if we help them prioritize, if they remediate one, it has a residual effect where some of the lesser controls are also remediated at the same time. And then we help them work to get their scores in SPRS and get them going down the right path of cyber maturity. So once that is done, they are ready to meet that requirement when CMMC is actually signed into law because CMMC once its signed into law, at the core, that's going to be the, you know, compliance with NIST SB 800 171.

Steve: I was going to say, why don't you go ahead while you're talking, Dan, to elaborate on the, the three legged process that we put their companies through.

Dan: Well, when we come in and do an assessment, we assess not just the technology or we assess the people processes and the technology. And the weakest link in the kill chain is the human end point or the people. So that has to be incorporated into the overall assessment and the processes, those are driven by the people. So processes that need to be incorporated are if they're, if the organization ever had an incident, you know, what is their response to that, action. And we help them to develop that in the process, as do they have a business continuity plan. You know, can they stay in business if they lost or their whole network and continue to operate, which is in addition to safeguarding the CUI data, all that goes into the overall assessment and those feeds and those all feed into those controls anyway, and that people, process, and technology is plugged into a cybersecurity maturity model that we implement, which has three phases and five steps. And we've it's a proprietary model that we've developed over the last three years where we can take an organization who currently is under the DFARs requirements, but eventually may potentially be a CMMC level three maturity when that's defined. And if they're following our process over time, their program's going to mature more to that level as they implement the different phases and different steps of our model. And what the organizations need to understand is it's not a one and done when it comes to cybersecurity and it's not a one and done when it comes to CMMC. Eventually, once the program started, it's to perpetuity. You all you got to maintain that program. And as you're maintaining that program, when you move into the higher levels of our model, you're testing your controls to make sure that they remain secure. Or they remain in place. And based on the results of those periodic tests you're collecting lessons learned and then now you're applying a process improvement to that and you're documenting it as you go along, because under the CMMC, there's a requirement to show maturity and it all has to be documented because when it comes to the audit side of things, the auditor could care less what technical control you have in place. He wants to see all the paperwork and if you don't have all the paperwork showing that you have a policy or procedure that dictates why you have a multi-factor authentication control or technology in place, it regardless if you have it in place, if you don't have the paperwork to back it up, you're still not going to you're still not going to pass that control.

Patricia: Why is it important to start the process now, considering that they don't have it all fleshed out yet?

Dan: So let's go back to this regulation has been around for the last ten years. And if you dig deeper into the DFAR regulation, they already are supposed to be meeting the compliance to 110 controls and 171. But what they don't realize is DMDC, what the federal auditing arm of this regulation can at any time they feel like it they can knock on the door of any organization and conduct an assessment right then and there. If they don't do anything now, they're at the risk of, you know, unannounced auditors showing up on their door where they're going to be assessed. And if they haven’t been proactive and started down this process, it won't be a good day for them. And being proactive and starting to understand where the gaps are and start chipping away at implementing those controls is vital to, you know, protecting that data, protecting our country. But it also gets you three or four or five steps ahead of one when the requirement does come down. So now you're not scrambling at the last minute trying to get ready because you just won this $100 million contract and the government's not going to release it to you until you meet that requirement. So we could say or talk business reasons wise, cybersecurity reasons wise. But there's a whole list of reasons why, you know, getting started right now would benefit

you. And two, the old adage is being proactive is always cheaper than being reactive. You don't want to, you know, have to implement something after the fact because it's always more costly with time and resources and finances in it.

Steve: To amplify a little bit more on that. Change is always hard in implementing this program. There's going to be a lot of changes to come about how people conduct themselves on their systems, how systems are being run. So there's a whole a whole gamut there that has to be looked at and, you know, and the reluctance of the people who work at these companies and their inability or unwillingness to change comes into play. So if you give yourself an opportunity to start today, when these programs do kick in specifically with CMMC, it won't be so foreign to them to make the necessary changes in how they conduct their operations or the conduct the way they do business. So it's easier, like Dan said, to be proactive to a situation and to react to it, because again, reaction is one of those things that people are very reluctant to implement because, you know, be like changing from one windows, you know, Windows 7 to Windows 10 or to Windows 11. Change is hard and people just don't want to do it.

Patricia: Very true. Very true. Well, I know you guys are going to be smartening us up on this whole process and what we need to be doing, especially from these webinars that you hosted. Is there any information that you'd like to share with our guests about any upcoming CMMC webinars you guys are hosting?

Dan: Periodically, we host our webinars around penetration testing and Zero Trust, and we have a webinar here that we will be scheduling with the last part of March that will be an overarching cybersecurity webinar that we will be hosting.

Patricia: Well, thank you guys so much for joining us at our Seaside chat. I'm going to be looking forward to learning more about CMMC at the next one and be interested and very much interested in the webinars that you're hosting.

Dan: And Patricia, if anybody's looking for information, they should go to the Cybersecurity and Infrastructure Security Agency at www.cisa.gov. That is probably the single best source for information around cyber security

Steve: Or Patricia they could go to www.firstteamcyber.com.

Patricia: That's where I go.

Steve: Yeah. And they can pick up our phone number, give us a call and we'd be certainly more than happy to answer any and all of their questions concerning CMMC or the DFARs law. Like Dan mentioned, know, we are very well versed in it. We have 60 plus almost 70 years of experience working in it and dealing with it. And again, we are more than happy to take the time to answer their questions that they want any and all questions they might have.

Patricia: That sounds great and we'll make sure that we send people with those same questions your way as well. We want to make sure everybody's getting the right information that they need out there.

Steve: Yeah, and that's one of the things. So I'm going to leave it at this, that's one of the things, Patricia, that Dan and I, we talk about this all the time and we call it witch oil salesmen. You know, a lot of these

companies will go out and see these advertisements that certain things will get them secure. And, you know, and we can laugh at it all day long. But what if they're led into believing that, say, you know, two factor authentication will get you secure or make your network secure? That's a misnomer. And the sad fact is that there are a lot of companies out there that sell that to their vendors and they believe it. You know, willingly or not. And that's not again, that's not what we do. We try as best we can to give our companies and the companies that we work for an assessment. And I and I always say this to everybody. I said this when I was in the Navy talking to commanding officers and that First Team Cyber is about doing constructive work for the company, not destructive. In other words, we're there to give you advice on what's going on, and we're there to help you, you know, fix those or remediate those issues. But if you look at what we tell you in a destructive manner, well, we both lose because the company is not going to be wise, will be reluctant to change. And we didn't accomplish what we were there to do, and that was to put them on the right cybersecurity path. So we know we we're honest brokers, you know, two Navy veterans. We believe in doing the right thing for companies. That's what we're all about. And that's what we want to continue to do. And again, if companies are willing to reach out to us, we will certainly work with them in making their cybersecurity needs met and putting them on a path to success.

Patricia: Well, that sounds fantastic. It was wonderful chatting with you both, and I'm looking forward to the next one because I'll have another round of questions to fire off at you.

Steve: I for one, Patricia, want to thank you and Giesler for allowing us to take the opportunity to speak with you today.

Dan: Patricia, thank you very much. Look forward to our next chat.