Podcast Episode 2- CMMC

Olga Torres: Thank you for joining us for the Torres Talks Trade podcast, where we discuss timely topics in trade national security, cybersecurity and supply chain issues.

Hello and welcome to the Torres Talks Trade podcast. Today, we will discuss cybersecurity and specifically the cybersecurity maturity model certification. My name is Olga Torres and I'm the founder and managing member of Torres Trade Law a national security and international trade firm. We have Dave Gray, our cybersecurity consultant. He specializes in everything related to cybersecurity and specifically CMMC certification. Thanks for being here, Dave.

David Gray: Well, thank you for having me, I appreciate it.

Olga Torres: Today, it's a very timely topic. One, because we are getting a lot of questions on CMMC and implementation deadlines and things like that, but also for everything we hear in the news regarding cybersecurity. If I remember correctly, the FBI reported in around 2020 that there was a 400% increase in cybersecurity attacks, and 400% increase sounds almost made up, and a large percentage of those cybersecurity incidents apparently dealt with ransomware. And, if people are not following cybersecurity very closely, there have been incidents where foreign hackers, for example, hack into American companies and not only they hack into American companies, but they go undetected for months. And in some of those cases, there have been situations where even US government agencies are subject to these attacks by these foreign actors. And some of them apparently involving actors in Russia and some other countries. I know there was another instance that involved the hacking of a pipeline and apparently it halted apparently 40% of the fuel supply in the United States. And the president ended up declaring an emergency which resulted in an executive order related to cybersecurity.

So, a lot of various different types of attacks, and it almost makes you feel, especially if you're a smaller business, for example, if the US government is getting hacked, what are our chances here? So that's why it's so important that people pay attention to these things. And specifically with things like the CMMC, even if you're not a defense contractor or a government contractor I think we can draw a lot of information and use that as a best practice for your organization as well.

I guess to get started, Dave, if you can give us more on your background and the kind of work that you do, that will be great.

David Gray: All right. Well, as you said a moment ago, my name is Dave Gray and I do work as a consultant, an assessor, and a teacher on a lot of things, just either general cybersecurity to include certification courses for security, like CISSP and security plus. But for the past couple of years, I have focused quite a bit on the Cybersecurity Maturity Model Certification, the CMMC from the well, it's based on a NIST program, that National Institute of Standards and Technology, but the Department of Defense, DOD, has adopted it as a way to demonstrate that vendors for the DOD referred to as the defense industrial base, or the "DIB," to ensure that they are in fact, protecting the data that the Department of Defense entrust them with.

As part of my participation with CMMC, that was fortunate enough to become one of the first 150 or so security assessors right now, we're still referred to as provisional assessors because the official certification exams have not yet come out. I also was able to extend that into becoming one of right now, only about 70 or so instructors specifically for CMMC and I used that background with organizations such as Torres Trade Law to provide consulting, assessing, and teaching. As I work with customers, I focus pretty much on what I would refer to as a coaching and mentoring perspective, because the DIB includes a large percentage of organizations that aren't quite ready to jump in whole hog, both feet, et cetera. Because it can get pretty expensive.

Olga Torres: Right.

David Gray: But by establishing that upfront coaching and mentoring process, then we gain a lot of ground and a lot of understanding without having to spend a huge amount of money. The rest of my background is basically from working with military and federal and state sectors. I retired as a Lieutenant Colonel and IT manager from the Texas Army National Guard. I spent about a decade with the largest or one of the largest state agencies in Texas and established a security program that's built on the same foundational areas as CMMC. And then again, most of my consulting, assessing, and teaching at the moment is in fact, focused on the CMMC process.

Olga Torres: It's really interesting that you mentioned costs, and it is expensive and, especially and we'll talk about it later, I think it's also delayed some of the implementation of CMMC and you can weigh in on that, but, I always think if you do get hacked, what's going to be more expensive for you to defend: the hacking instance, incident and having to deal with the reputational, followed, having to tell your customers that you were hacked or in some cases you cannot even access your own data or your systems. That's when there are certain costs that at some point you just cannot avoid. And I think cybersecurity, it's definitely one of those that should be top of mind. So, in terms of top cybersecurity concerns for people that are not very well versed with cybersecurity, other than what they hear in the news, what are the top cybersecurity concerns in 2022, in your opinion?

David Gray: Well, of course, opinions vary from one person to the next. I would say that the top two concerns, and this comes from a business background as well, is the ability to continue running your business. And in order to do that, the more susceptible areas that businesses fall victim to can be pretty much bundled into two topics. One is ransomware and the other is referred to as “BEC,” or “business email compromise.” So, with ransomware, a lot of folks have heard about that. It is kind of one of those splashy things that comes up on the news and in most people will have at least a vague idea of what that means. Generally, it includes an organization that has been compromised to some extent, so that a malicious actor. Now, when I use the term malicious actor, I can also use the word bad guy. Sounds more professionals saying malicious actors. But those malicious actors are primarily in two different categories. By far, the largest is cyber-crime or cyber criminals. A much smaller percentage, but just as impactful, especially as it relates to DOD data, are nation states. Now we're talking about, China, Russia, North Korea, and in some cases, Ukraine, they all lead the parade, so to speak, as having had the greatest impact from a cyber-criminal perspective.

Now, from a CMMC perspective, we're talking specifically about data that the Department of Defense has entrusted with defense industrial base vendors. And so those companies have, essentially by virtue of a business decision, to work with the DOD, to some extent they've made themselves a target and that target is going to be from a percentage-wise greater for everybody else when it comes to nation states.

So, if you've read or seen documentaries about the, one of the most expensive jets ever created by the US Air Force, the F-35, within a year or two of that jet becoming operational after decades and billions of dollars of research and development, China had the exact duplicate. How did they come up so quickly with that exact duplicate? They stole data from the Department or from defense industrial base vendors and in some cases from the military itself. And so, we, as an organization, excuse me, we, as a country, are spending additional trillions of dollars in research and development to stay ahead of our adversaries. Primarily because our adversaries don't have to spend that R&D if they can take the cheaper, more efficient method of just stealing the data and then replicating what we've already done.

The other item I mentioned as far as a significant issue for 2022 is business email compromise. Now, what is BEC and exactly how does it impact folks? It impacts folks because the malicious actor in this case is impersonating some type of senior leader or executive with an organization. And they are sending impersonated messages to their own staff. Or at least the malicious folks are sending messages to the organizational staff in primarily two areas. One is HR and one is Finance. So, okay well, why HR? Because HR is the repository of personal information for an organization. Personal information is incredibly valuable when stolen and placed for sale on the dark web. The other area, Financial, is when a BEC email goes to as an example and accounts payable, clerk, accounts payable clerk may not have been receiving sufficient training as it relates to recognizing these spoofed emails and typically those emails are providing a direction of a last-minute change.

So, as an example, at a company, not a company, but a small city just south of Austin in Texas, they had their contract department, which was paying for road paving. Road paving doesn't sound very exciting but when you start paying the bills is in the millions of dollars, it's very expensive. And so, a last-minute email comes in and says, oh, the company that we've contracted with and we owe $5 million to, they just recently changed their bank. So here use this routing number and account number instead of the one that you have on file. And then that city lost millions of dollars because the accounts payable person had not yet been trained properly, inadvertently believed the email and made the changes without double checking with the appropriate individuals within the department.

Olga Torres: You know, that's funny that you mentioned that impersonation. I remember a couple of years back (and we were pretty good at training in terms of cybersecurity, and we're small), but there were a couple of months where it was happening a lot. And I had people call me and say, “You just emailed me.” And it was basically, it looked like my exact same email but if you check with your phone, you can't really tell the domain name is different. It could be olgatorres@gmail.com, but if people are checking in the morning or quickly, or they don't pay attention, they just see the name coming in and it was something like, “Are you in the office?” and they will do it where even it was like around 7:30, 8, people are getting in and that they would just assume it was me. It's training; it's so important for people to double check before replying, especially if there's anything like, “Hey, can you send me a wire? I really need.” And this happens a lot.

It happened to one of our clients where even though the company, for example, apparently had procedures to double check before sending wires and doing different steps to double check identities in this case. It wasn't done, so even if after the training and even after you have procedures, it can still happen, right? Human error. It's so important. Let's talk a little bit about CMMC and the framework, and, and even if you're not a government contractor, why should people care generally about CMMC?

David Gray: Within the government environment, one of the key drivers is compliance and if you don't comply with the rules, then you can't play the game. You essentially have to just pick up your toys and go home. For a cybersecurity professional, I recognize that compliance is incredibly important. I've got an MBA in business; I'm aware that organizations have to make profits, but I'm also aware that organizations, if they can't stay in business, well, then they go out of business.

Olga Torres: Right.

David Gray: And as we mentioned two of the larger issues to address in the near future is the issue of ransomware and the issue of business email compromise. Both of those can entirely cripple an organization. When it comes to security in general, we as a global planet interact with each other across the world, being on the internet doesn't restrict your transactions to someone in the same city. It could literally be anywhere on the planet earth. Any organization that has anything of value can be subject to criminal activity, trying to steal that information. Why CMMC plays into that very well is that, originally, CMMC was based on a federal set of rules and not being federal agencies when the Department of Defense decided to transition their defense industrial base in two similar rules, they made a subset, literally one third of the federal rules coming up with what are now known as the 110 practices for CMMC. Those practices are geared explicitly for non-federal organizations in ensuring that data confidentiality is achieved and maintained.

As a set of guidelines, those 110 practices, which equate to 320 assessment objectives become an excellent foundational area that organizations can focus on. In fact, they use the word "foundational" within CMMC to delineate between a couple of different levels of organizations and the type of data that they are trying to protect. Level 1it's literally the 17 or so practices from the NIST 800-171 that exactly mimic and match the Federal Acquisition Regulations requirement for simple, basic security. So, even if you're only focused on things like purchase orders and your own organization's data, then that level one, those 17 controls are...

Olga Torres: Can you give us example of what those are, those 17 controls?

David Gray: The controls are a variety of controls based on domains of security. The domains include things like the, the access domain or the configuration management domain or the identification and authentication domain. And as we look in detail at those controls, the basic controls such as establishing who can access what data is foundational to any organization's control of their own data, whether it be confidential or not. As an example, most organizations that are large enough to have a human resources or HR department also have data that is extremely valuable, it's referred to as PII, "personally identifiable information," and that data is accessible (and rightfully so) by persons in the HR department whose job role and function is to deal with that. But that same exact data in the same organization is actually no one else's business. It's not a person that's in the manufacturing department's business. It's not a merch person in the financial department's business or the engineering department's business. Each of those organizations need to segregate and apply data controls based on what type of data that they deal with.

Another example, in addition to HR, would be engineering, research and development. Research and development is proprietary to individual organizations and is extremely valuable to other organizations that are in a competing market. And so, organizations would be to their advantage to at a minimum look at those 17 foundational controls. Now subtract 17 from 110 you get 93. The other 93 controls, at least as far as the DOD is concerned, those are controls for sensitive data referred to as CUI, "controlled unclassified information." The Level 1 controls reflect FCI, "federal contract information," the upper-level controls, Level 2, are controlled on classical information. That's the type of data that the nation states are really after. They're not so interested in a Level 1 piece of information, like a purchase order number, or how much a particular client paid for a particular deliverable, whether it be a device or software or service. But they are extremely interested, the nation states are extremely interested in data on, as we brought up earlier, how to build an F-35 fighter jet.

Olga Torres: Export-controlled technologies and things like that.

David Gray: And ITAR- and export-controlled are also categories of CUI. So, yes, they have similar control characteristics. Overall, there are around 80 or so CUI categories and most organizations that deal with DOD will participate in at least a handful, maybe a dozen or so of those categories. And then part of what we as consultants do is we identify where the data is. In fact, our motto is "follow the data." And so, our very first conversation with any person, any organization that's interested in protecting their data is to scope where that data is and where that data flows back and forth. Does it flow just between a customer and the client? Does it flow between a prime vendor and multiple suppliers at multiple levels of the supply chain? Does it flow to a cloud service provider organization where at each step and each location that data must be protected. And due diligence says that you trace where that data goes and where it comes from, where it exists, where it travels, where it's at rest in place, appropriate controls in place to ensure the confidentiality of that.

Olga Torres: Yeah. That's really interesting when you mentioned, for example, CUI and export-controlled information. That's some of the cases that we've worked on. In addition to assisting companies with CMMC certification, for example, there have been instances that there's a little bit of an overlap or crossover between, let's say you have a cybersecurity incident, and your ITAR or your EAR data. And I know I'm throwing acronyms, Export Administration Regulations-controlled data is compromised then you get into situations where should you consider Voluntary Self Disclosures with the various export agencies and what are the pros and cons of doing that? So, it's a little bit of a crossover in our worlds there.

Okay, so let's talk about the CMMC implementation date and, I remember these from 2017 and back then there was a deadline. I remember we were assisting a lot of clients trying to revamp their cybersecurity and they had the plan of action and various things. And then slowly but surely has been moved over the years and now we're at a different implementation deadline. What's the new implementation deadline or at least a targeted date and what happens if companies are not ready by then?

David Gray: Alright, so just to provide some context and you mentioned 2017, as a key date. At the latter part of 2017, we're talking November, December and which by federal guidance is in the 2018 fiscal year. Contracts with the Department of Defense, under DFARS, so we've got the Department of Defense Federal Acquisition Regulations Supplement, began to include requirements to protect data. The bottom line is that it basically said use the National Institute of Standards and Technology special publication 800-171; that's where the 110 controls come from. And so effective that date, all DOD vendors were accountable to having implemented all 110 practices, but that didn't happen. DOD recognize that didn't happen because their goal was to slow down the data theft and they realized that many organizations didn't have sufficient expertise for understanding those 110 controls.

In 2018, they adopted another NIST document. This was the assessment document for the 171 referred to as a 171A that included an additional 320 clarifying assessment objectives. But then again, the DIB was not being held accountable contractually. As a result, many of the DIB participants decided to delay or not meet those particular terms and conditions. There was apparently no downside to that because there was no accountability whatsoever. When DOD recognized that accountability was the only way to enforce the requirement, they implemented CMMC, which took those 110 practices and the associated 320 assessment objectives and turned them into an auditable requirement. And not just those, it actually had 20 additional controls added on top of the 110. Well, at this point, when you can imagine. If you go to the store all the time with your kids, and every time you pass by at the candy counter, you hand some candy to your kids, they get accustomed to it. Well, you have to become accustomed to not being held accountable for those controls. And so now that they were about to be held accountable through independent assessments, there was a lot of push back.

Olga Torres: Right.

David Gray: And that was reached all the way up into Congress. Congress reached over into DOD and basically said, "Why are you doing this?" And the explanations went back and forth and from a logical perspective, they all make sense. But from a customer expectation perspective, from a customer relationship management, CRM [Customer Resource Management] perspective, and that's what the DIB is for the DOD, they are basically the DOD is a customer. The ability to keep that relationship working is absolutely critical. For the future of the United States Department of Defense. And once the DOD received feedback that said, this is considered a surprise, even though DOD says, oh no, you've known about this since 2017, they backed off. DOD backed off and they said, look, we will reevaluate CMMC. And what came out of that re-evaluation in November of last year. November of the year, 2000 and what years now? Yeah, 20. So November last year, CMMC version two came out. Now what that did, it tried to allay some of the fears from the DIB, as far as the DOD, having tried to implement overreach by adding controls. And so, essentially what's CMMC 2.0, does, is it goes back to a straight, plain vanilla NIST, special publication, 800-171A.

But there's still a lot of pushback. Why? Because this is going to be incredibly expensive for organizations that have not previously invested in cybersecurity to implement. DOD still has a very large lack of empathy, put it that way because they'll say, "oh, well, you've been required to do this, then we're not gonna be bothered too much about the fact that you're complaining is expensive." In fact, DOD is saying that there should be no cost. And there's the reason they give for no cost is because they're saying you've been signing contracts for years stating that you already meet those.

Olga Torres: Yeah.

David Gray: So now everything is up in the air and the biggest word that I tell people to remember, and this comes from my 32 years of experience in retiring as a Lieutenant Colonel of the Army, is patience, right? Because nothing happens quickly in DOD, absolutely nothing. Where does that leave us with CMMC today? Today, CMMC 2.0 is the law of the land, but it won't be implemented until rulemaking is complete. Now what is rulemaking? Rulemaking is where the acquisition rules for the federal government and the Department of Defense are analyzed carefully to determine the impact on, in this case, the DIB, and to understand the costs on all sides. There're costs to the DIB to implement; there're costs to the DOD to lose critical data to data theft.

The expectation is that rulemaking will be complete in about the middle of this coming calendar year 2023, maybe a bit earlier, maybe a bit later. But at that point CMMC will begin appearing in new DFARS 7012 clause contracts. Now, why do I slow down and emphasize that so much? If you have an existing contract, this is not retroactive, it doesn't go back and change your existing contract. The only thing that's been changed relative to current and existing contracts is that organizations in the DIB must conduct a self-assessment using the Department of Defense assessment methodology, which applies a scoring matrix to those 110 controls. That score as a self-assessment maybe by experts, maybe not, will then be recorded in a Department of Defense database called SPRS, "supplier performance requirements system." That score starts at a perfect level of 110. If you have all 110, everything's fine and not just the 110 practices, but all 320 assessment objectives, then you're great. Once a year annually, a senior leader within the organization must ensure and take accountability for updating and maintaining that SPRS score.

But what if you're not perfect? Well, there are penalties in the way the scoring is done. You either have a penalty of a negative one, a negative three, or a negative five, and an organization that absolutely has all the penalties will literally have a score of a negative 208.

Olga Torres: Have you seen a lot of those?

David Gray: I have, I've had a lot of organizations that felt that they were in the positive 70 to 80 range, but when we've validated their scores, the last two clients I did that with one was a negative 130 and one was right around zero. And on average the scores are about a negative 150 to a negative 100. And how do we know that? Because there are organizations under the federal government, under the DOD, specifically the DCMA, the Defense Contract Management Agency, which has what's referred to as the DIBCC the Defense Industrial Base Certification Center that organization has discovered that 75% of the companies that they've assessed, who claimed that they were perfect, 75% failed.

Olga Torres: Yeah.

David Gray: So, it's very complex when you get into the minutia of those 320 assessment objectives. And again, though, from my MBA perspective, what's the impact when the DIB, well, there's a couple of different impacts. Firstly, if you don't have an SPRS score on record, then you will not be able to participate in future contracts. This is the only retroactive area as well. So, for instance, if you have a contract with four option years, so the total contract length is five years and you don't have a score within the appropriate timeframe, annually. Then when the contracting officer for the military department Air Force, Navy, Marines, whomever, they will literally deny you the ability to take that option here. Now for new contracts, same thing. If you don't have a score within the last 12 months entered, then you will not be able to participate in your application where your, your proposal will literally be discarded.

Olga Torres: And right now, as long as you have a score, right? Even if your score is not the greatest, as long as you have a score?

David Gray: Technically, if your score is a negative 203, then yes. You could still get a contract. Now having said that, having said that, the contracting officers. . . Although there is no formal guidance yet to implement or integrate scores from SPRS into award selections. We know that that happens because if, if I'm a contracting officer and I see competing companies, and one of them has an outlandishly horrible score, and I am concerned about the data confidentiality, then I'm not going to select that company. And then if the other two companies are equal upon every respect, the equal in price they're equal in quality, they're equal in background, then that score may become a differentiating factor where you don't have a bad score you just don't have one as good as your competitor.

Now what about the actual CMMC? What I've been talking about for the moment is SPRS this supplier performance requirements system and that is mandatory on an annual basis, but the CMMC does not yet exist. And the

Department of Defense knows that they cannot on whatever date may be the middle of this coming year, 2023 or not, they cannot like a huge sledgehammer, just start adding CMMC to a hundred percent of future contracts. So, DOD will pick and choose contracts that have data that they are more concerned about. And those initial months, or years of contracts will be the first ones to have a CMMC clause added to the contract.

Originally, the DOD plan was to phase in CMMC over a period of five years. We've already blown past all of their milestones and expectations, and they've all been left, just sitting in the dirt because nobody has been able to really perfect the CMMC program, yet. So, what does that mean for you the DIB. It means that in 2023, if you are perusing through future contracts, you may find some that includes CMMC, you may not. Within two or three, maybe four years after that, it'll likely be a hundred percent. And what does that mean for you, the company that it says you have to be CMMC? It means that you will need to have provided, based on whether it's an FCI federal contract information only or CUI controlled unclassified information, you will be held accountable for having the correct assessment and certification.

At level one, FCI is a self-assessment: you follow the instructions, and you document that you went through and created the score, that may or may not be accurate if you have, or don't have the appropriate expertise. That will impact a little over 200,000, maybe 220,000 vendors.

The Level 2, however, which impacts organizations with CUI, currently estimated at around 80,000 organizations, they will need an independent assessment from an independent assessment organization known as a C3 PAO. It's the DIB’s partnership with a nonprofit organization to coordinate the entire CMMC infrastructure across the entire country. And, at the moment, there are only about a dozen C3 PAO companies that can actually consider themselves qualified to do those assessments.

So, moving forward, the DOD has a large challenge to increase the number of those assessment companies, because you can't take 12 companies and divide it very well into 80,000 DIB vendors and have any sense of ability for success. This is all up in the air now. What was my favorite word for all of this again? Patience. Because we can continue to expect disruption from everything that we're seeing, but we can also expect that eventually it'll all get worked out. Does that mean that we can ignore it for now because we don't think we're going to be impacted for two or three years? Well, consider this, if you're starting from scratch, it typically takes 18 months to two years to get to the point where you can be successful. So, if you've got a year and a half to two years of preparation and you have any indication that you'll be held accountable within that timeframe, then today's probably the best day to start.

Olga Torres: And also, I would think you can stretch out your expenses right over a period of years, rather than you have to implement everything in a few months.

David Gray: Well, it certainly depends on the business expectations and the type of data. And keep in mind that security is considered a valid expense under a DOD contract. So, if you ensure that in your proposals to DOD, that you've identified line items that reflect additional security costs, then those will be considered acceptable costs. And so, you can essentially be reimbursed from DOD for your costs.

Now, having said that, if you don't define explicitly what those costs are, you cannot go back and recreate your contract. You cannot go back and recreate your application for proposal, right? So, you're pretty much stuck at that point, but moving forward, get into the habit of identifying your security-related costs and expenses and put those down as separate line items in your proposals. So that you prepared your business environment to gain as much reimbursement, therefore value out of your relationship with DOD as you possibly can.

Olga Torres: Great. Well, this is all very useful information. Dave, thank you so much for your time and thanks to our listeners for tuning in today. I feel like this one deserves a follow-up in, in the next few months. Thank you.

David Gray: Yeah, things will change. So, a follow-up in a few months will be perfectly appropriate and I appreciate you having me on your, on your program.

Olga Torres: Thank you.