Ray Thibodeaux : Welcome to Keys to Winning, a podcast where we talk about government contracting topics such as proposal development, business development, win strategies, and more. Keys to Winning, produced by AOC Key Solutions, a leading bid and proposal development firm gives you a chance to learn from leaders and experts in their fields. I'm Raymond Thibodeaux, today's host of Keys to Winning. Today we talked to Victor Marchetto about the growing concern over cybersecurity and federal contracting in a fast evolving cyber threat landscape. Victor is an information security expert for CDW and it's a topic that's gaining more urgency with data breaches and cyber fraud becoming more common as hackers and their technologies become more sophisticated. A recent report from the Government Accountability Office found that almost all of the US military's newly developed weapons systems suffer from mission critical cyber vulnerabilities some were even described as easily exploitable. Scary thought. With that, thanks Victor for being on the podcast. I wonder what people who are in the business, what is it that they're most concerned about when it comes to cybersecurity in the federal sector?

Victor M.: Cybersecurity in the federal sector has a lot of the same problems that cyber security has in any other sector. Much of what industry leaders are concerned about is just the myriad sources of different threats to your organization and how to craft a complete and well rounded response to what the world presents companies these days.

Ray Thibodeaux : One of the things that I've notices is that there are probably some agencies within the government that are more prone to hacks and data breaches than others. I think the one that really comes to mind is the IRS and they hold this trove of personal information that is fairly lucrative in the wrong hands.

Victor M.: Yeah, certainly is. Those are the obvious targets, right? There was a large, now very famous, breach at OPM that dumped a ton of credentials and information about anyone that has a clearance or has undergone an investigation, and that was a treasure trove of information for whichever threat actor was responsible. I don't know if they've nailed it down yet. It's good for agencies and people working for different federal customers to consider, you know, "Hey, what do people want that I have?" Or, "What kind of information am I privy to that might be of use to someone maliciously, and what could someone use this data for?" It's also important to think about who do I have access to by the nature of my job or my connections.

Victor M.: A lot of times when truly the professionals in, be they state funded actors, or highly organized cyber criminals. They're looking for ways to circumvent all of the defenses that agencies will deploy and they'll look for these trusted relationships with third party entities. Smaller agencies that have connections in through to larger agencies or contractors are often targets. You may not be the end target. I don't think anyone can say anymore that they're too small to hack.

Ray Thibodeaux : It's interesting that you say that because what I've noticed in the last few years, especially is that going to different federal contractors, you notice that there is a lot of focus on information security within the organizations. A lot of times they'll send out fake phishing emails and they want to see what percentage of their organization actually responds to that and maybe downloads a fake virus or whatever. Then, you get a follow up email afterwards saying, "Oh, you should have paid attention to this, that and the other thing." Aspects within the email that would have tipped someone off that was being slightly more vigilant that this was actually a phishing email. The reason I asked that is because with all of the software and all of the cyber defense tools that we have, it really does come down to the employees are the best defense against that. Is that still true or is that not the case?

Victor M.: I would agree that that remains true. Any sufficiently funded, a sufficiently trained, sufficiently motivated attacker will get into your system or your network given enough time. Now, that sounds really bleak. However, that doesn't mean that the defenders can't win and that we can't protect our own, our customers, or our government's data. The harder that we make it for them, the more money they have to spend, the more time they have to spend, the greater chance that they can be caught in their actions and dissuaded from attacking further. Like you said, the users are oftentimes some of the easiest vectors into the systems, right? A lot of these attacks find their first chink in the armor in the overall organization through a cleverly crafted social exercise, right? If you get that email that says your Amazon two day package is arriving, here's your tracking number, click this link and you click the link, even though you may not recognize that particular email or order or something, right? We're not reading all the headers and we're not seeing all the technical controls to verify that it's the exact same email that we were expecting. Right.

Ray Thibodeaux : We've all ordered from Amazon, so it doesn't seem all that out of place, that "Oh here is your tracking number." Yeah, it does require, it seems like a lot of vigilance and things to look for, which leads me to the next question. Not to get into the politics of it, but when the Democratic National Committee was hacked, whether it was Russia or whoever, I think the indictment actually claimed Russia. I think what I found interesting about the actual indictment was the ways that they were able to gain access through what was known as spear phishing and spoofing. Can you kind of explain what those are?

Victor M.: Sure. Phishing is a tactic used by malicious actors or hackers. It's used by them to get the user, the target, to click something which will request a file or something. It begins the whole attack chain and it brings the payload to them. Then once they click on that link, it kind of lets them in and lets them move on with the rest of the phases of their attack, which can be very detailed and very complicated I guess is what I'm trying to say. Spear phishing is when someone targets a specific person, it's when they send an email to a specific person and

they craft it just for that person. They will often do a lot of research and gathering open source intelligence of things on your Facebook, things that are publicly available information about you if you're the target. The next step after that oftentimes is to spoof or to act as if you were that person.

Victor M.: Let's say I'm a hacker and I send a very targeted email to the CFO for example. The CFO, I do enough research about him and I send him a news article that he's really into pens or cigars or whatever it is, and he clicks through to see the latest update from Cigar Weekly, or Cigar Monthly, or something. In that process, I can do some technical wizardry and gain access to his email and gain the credentials of his email. Now the next phase of my attack begins and I pose as the see the CFO. After listening and watching and collecting his emails, I can then craft an email to the right people in finance and have them wire transfer money to an account, and since it's coming from someone that they believe to be the CFO using his words and using his mannerisms, they're more likely to wire money to that account.

Ray Thibodeaux : It seems like we've come a long way from the Nigerian prince with 300,000 barrels of oil and need your bank account number.

Victor M.: That's right. It's important that people doing this self auditing. It's also important for organizations to to enlist the skills of the dispassionate third party. My company, I'm a part of a team that has a team of white-hat hackers, ethical hackers, that can do these assessments or run these type of phishing campaigns against your users so you can see exactly how your defenses are working and who your repeat offenders are, who understands how to spot a phishing email and who knows the proper protocol about what to do about it. It's something we always tell our customers. It's much better to find out about your weaknesses from a friend than from your enemy.

Ray Thibodeaux : Totally. You had mentioned earlier in the conversation about state sponsored hackers, we always hear about a lot of these back-door microchips, like say, Lenovo Computers, which is a Chinese company and there have been some hesitation on the part of some government agencies to order anything from Lenovo, because I thought that there was some kind of a back door to that device, so that they could spy, basically. The same thing was going on with Android phones. I mean to what extent is that actually happening and how much of that is just maybe urban legend?

Victor M.: Right. It's definitely a great fear of many of many companies, of our government, of many governments that the hardware, the technology that they need to do the work that they're doing, you know, to everyone, the technology we use to do our jobs could betray us in some way. Right? It certainly makes for good television, but there is a kernel of truth in all that. There's recently been a journalist who reported on the potential that Super Micro Servers, which is,

Super Micro is a well known server manufacturer. This researcher was able to track the manufacturer of these motherboards that the servers run on back to a point where they may have been introduced or modified with special chips that allow a backdoor to whoever installed them. If through intent or through just mistakes or bugs in software can allow third parties to access machines, your software, your phone, whatever it is. It's a real possibility.

Victor M.: I mean it could happen, and that's why a lot of RFPs are having components about, "Tell us about your supply chain management, like how do you evaluate where you're getting your products from? How do you verify that they haven't been tampered with in the process?" It's something that we should all consider when building these large IT systems. "Where's all this coming from?" You know? Has anyone verified the code that we're installing or the code we're about to disseminate to our customers?

Ray Thibodeaux : Part of what interests me about that is, I think we had talked about this a little bit earlier, there are plenty of standards and protocols for ensuring information compliance. There is FISBA and government guidelines or standards for information security and cyber security, but there doesn't seem to be an international enforcement mechanism. It does seem kind of alarming that in this day and age there's no United Nations or an Interpol type of thing.

Victor M.: Yeah, there's no Geneva Convention for cyber warfare. When you think about the threat landscape, why are people doing these attacks? What's the incentive to doing this? There's a number of motivations. There's espionage, you want information and access to information secrets and technology and whatever. You have a criminal motivation, which is really easy to understand. There's also another motivation, which is the activist motivation. There's a lot of causes out there that people feel very strongly about. Folks want to destroy organizations or movements that they are against, and so that could motivate someone to do this. People can take these actions in the real world where they are at risk for physical harm, but if you're doing it digitally, and you're doing it from Belarus, nothing's going to happen to you. What are the chances that the US, or the FBI, or whomever is going to knock on your door and extradite you to the US to face the music for your crimes? Not Likely.

Ray Thibodeaux : Do you think it's inevitable that there would be something like that in the future?

Victor M.: I hope so. I hope so, because we do so much commerce globally through the internet that we really should have something where we all can get together and say no one should attack critical infrastructure. There should be some rules of the road.

Ray Thibodeaux : Thank you, Victor. It's been a good conversation. We'll close there. I'm Raymond Thibodeaux, and this has been Keys to Winning, from AOC Key Solutions Incorporated or KSI, a consulting firm that helps companies across the country win billions of dollars in federal contracts. Learn more at www.aockeysolutions.com, or follow us on LinkedIn. Be sure to subscribe for more podcasts in this series, and thank you for listening.