Chris Riotta:

Hi, everyone, I'm Chris Riotta, staff writer for FCW, and I'm so excited to have you all here for our 2023 Cyber Summit and our first session of the day, Protecting Critical Infrastructure. The government's most essential and powerful assets are increasingly frequent targets for attackers. Electric utilities, water treatment plants, chemical manufacturers, hospitals, and even schools are all under threat. Now, more than ever, cybersecurity experts understand that an attack is not a matter of if, but when.

So this March, the Cybersecurity and Infrastructure Security Agency, otherwise known as CISA, announced a pilot program intended to identify vulnerabilities within critical infrastructure systems that are known to be exploited by ransomware groups and threat actors. So how will this impact the prevalence of damaging ransomware incidents? Here with me to discuss all this and more is Gabriel Davis, Risk Operations Team Lead with CISA. Gabriel, great to have you here.

Gabriel Davis:

Thanks so much for having me here. Wonderful to talk about this issue that we have going on in the country, what we're trying to do to drive down that risk, and hopefully make an important impact in securing the nation's infrastructure.

Chris Riotta:

Yeah, yeah. I'm really looking forward to learning a lot more about this pilot, but I first want to take a quick step back and kind of lay the foundation here. Can you tell us a little bit about your work at the nation's cyber defense agency, as well as maybe a little bit about the current threat landscape and how it's been changing?

Gabriel Davis:

Absolutely. So a lot of my work centers around making data-driven decisions on how we're going to approach the cyber threat landscape. And what that means is we're looking at what threat actors like, what types of vulnerabilities do they like to exploit, where do they typically go for these types of vulnerabilities, where the most prevalence is for these types of vulnerabilities, which devices have the most vulnerabilities in them?

So we can try to triage this in a way that makes sense so we're not just throwing everything we have at every problem all the time. We have some type of systemic way to go through and say, these are the problems that need to be addressed first, and then we can iterate our ways back through that. So that's a lot of the work that I do here at CISA is taking those, that data, and transforming it into a risk-based analysis to make decisions based on those vulnerabilities.

Chris Riotta:

Interesting. And before I go any further, I do want to make a quick plug to our audience that you can feel free to drop questions in the chat, and we will try to facilitate those the best that we can as we go forward with the conversation. But, Gabriel, I'm wondering if you can tell me a little bit about when it comes to critical infrastructure, specifically, where some of the biggest vulnerabilities can really typically be found? What do you see in your work when it comes to that?

Gabriel Davis:

So, unfortunately, there's no sector that is immune from vulnerabilities. Devices themselves in their manufacturing process, threat actors have all the time in the world to figure out how to break in and how to use a device in a way that it wasn't intended. So, unfortunately, as we move to more of a IOT, Internet of Things, system where we have this cyber and physical convergence, critical infrastructure operations are going to be more tied into the Internet of Things as we talked about, things that are going to be connected more to the internet, things that are going to be used in more remote capacity.

I mean, if we take just the pandemic, for example, we saw a large swath of the country move from on-prem activities to doing things from their homes, which isn't a horrible thing, it's not a bad thing at all. The problem is everyone's home infrastructure isn't rated the same way as, say, the business would be. So what we have is now we've expanded the exposure of the country's IT space, because we've moved everything in a more dispersed fashion, which, again, isn't a bad thing. It's actually a good thing, but we have to do it properly.

So, unfortunately, there's no one sector that's immune. All the sectors have their nuances, but what we're trying to do is we're trying to make sure that we're meeting the threats at the gate. We're outside of the network saying, "No, you can't come in," and making sure we take away those opportunities as opposed to waiting until they're inside the network and trying to evict them and recover.

Chris Riotta:

Yeah, it seems like such a complex thing when it comes to critical infrastructure since, as you say, no sector is immune. And then when you look at the network across some of these critical infrastructure sectors, like water, for example, a lot of that is across the private sector and in these really sort of siloed kind of small communities where there's only a few operators who are manning these systems. So I'm wondering if you can talk to me a little bit about the Cyber Incident Reporting for Critical Infrastructure Act and how that has kind of impacted your work and impacted critical infrastructure owners and operators across the country.

Gabriel Davis:

Absolutely. In a nutshell, what that Act does is it empowers both the agency and also private organizations to come together and to start sharing more information about these incidents as they happen and before they happen, so that way we can all respond a little bit better, a little bit more rapidly. The best approach to doing this, in my opinion, is going to be that community safety approach. Think about your Neighborhood Watch. See something, you say something. That way someone else isn't victimized.

And that's what we're trying to get with this Act. We want to be able to say, "Hey, Organization X was compromised by this vulnerability or by this threat actor. We know the things that they like. Let's go warn the neighbors within a similar sector that these are the types of threat actors that are coming for these types of vulnerabilities, and this is how you can defend yourself against them."

And that's essentially what this Act is going to do. It's going to facilitate a greater information sharing between the government and the private sector. We can't do this without the private sector organizations. We need their help. This is not going to be a government internal activity. This has to be something that has to be done across all critical infrastructure in a partnership.

Chris Riotta:

Yeah, and I know one thing that CISA has been really good at since it was launched back in 2018 has been forming these sort of partnerships and kind of collaborative working groups around some of these issues to tackle some of these biggest issues. Can you tell me now a little bit about the Ransomware Vulnerability Warning Pilot? Who's involved with it, and what kind of led to its formation in March?

Gabriel Davis:

Yeah, absolutely. So the Ransomware Vulnerability Warning Pilot program is something directly from the CIRCIA legislation. So as a part of it, CISA's been charged with going out and proactively identifying vulnerabilities that ransomware threat groups like to leverage. So think anytime you have a vulnerability instance, say Clop ransomware group back in early part of the year was leveraging some software vulnerabilities that they like, or Royal ransomware group leveraging other CBEs.

We'll say, "Okay, we know that these like these vulnerabilities. We've identified them in the wild being compromised. We can say with some definitive certainty that if you have this vulnerability, your chance of being compromised by a ransomware group as opposed to just run-of-the-mill exploitation is higher, because we know it's been done." And as we've learned through our research and work through the Known Exploited Vulnerabilities Catalog, the number one indicator on whether or not a vulnerability's going to be exploited is whether it's been exploited before.

So we know what we're trying to do is we're trying to understand better what they like so we can take that opportunity away. We're shaking the door handles, we're checking locks, and we're being proactive. We're actively looking for vulnerabilities. Gone are the days where we passively vulnerability scan at the perimeter and hope everything's okay. Those days are behind us. The threat actors are moving too fast, they're much more sophisticated. We're always going to be playing catch up. So we have to be just as proactive as they will. So learning what they like, taking that opportunity away from them, and that's what this pilot does.

And as part of the key players, this is a interagency organization or interagency program that's designed to be shared amongst a large group of government agencies and the private sector. So it's very conveniently nested between the Joint Ransomware Task Force, which is also a part of that legislation where we have... where it's co-chaired between CISA and the FBI, and, again, interagency working group where we're all coming together, we're sharing the information that we're seeing, we're sharing those IOCs, those TTPs, and everyone has a specific part to play, a constant deconfliction one. What part of the attack spectrum are we fighting?

The ransomware vulnerability warning pilot is as far left as we're trying to get. That's to the point to where there's not been a compromise, we have no evidence of a compromise, but you are at risk, because we know that these vulnerabilities have been used in the past.

Chris Riotta:

Yeah, that proactive approach makes a lot of sense. We got one question in the chat just asking to clarify the name of the law where this pilot sort of was established from. That's CIRCIA, C-I-R-C-I-A. It's the Cyber Incident Reporting for Critical Infrastructure Act. What I kind of love about the Ransomware Vulnerability Warning Pilot, I was telling Gabriel before this, was that for a government name of a project, it's actually very simple and sort of clear.

But if we can just dig maybe a little bit more into the weeds here, Gabriel, what does the work actually look like, and what are some, maybe, updates from the pilot so far? I know it only just kicked off in March. And then what is your team hoping some of its outcomes might be? Are you planning on publishing your findings, or are you going to make sort of these warnings accessible in some way? What are the goals?

Gabriel Davis:

So the number one goal is always going to be to drive down risk in critical infrastructure. That's it. That's the number one goal, however we can do that. So as a part of the kickoff of this, we made an initial round of notifications related to the ProxyNotShell vulnerabilities that are chained with the Microsoft Exchange platform. So what we found was that these were being actively exploited at a period of time earlier this year. So we said, "Why not start there?"

Typically, where we're prioritizing our work is going to be in those target-rich, resource-poor types of organizations, right? Think your small, your state, local, tribal, territorial governments, small and rural, medium-sized organizations, places that don't have multimillion-dollar budgets that can defend themselves effectively. And that's not to say that those folks don't get our attention as well, but we know where the troubles are.

Think that cyber poverty line. That's where we're trying to operate is how do we have the most impact where the most Americans are going to be affected? So water and wastewater sector is an excellent example. Highly decentralized sector with tens of thousands of individual municipalities running their own water treatment facilities. So that's a situation where we know we're going to have to be working in complete tandem with those on the ground and also those private organizations, and as well as the ISACs, to make sure we're getting the word out. We're spreading this information.

And also, hey, we make a notification, share this with your partner. Let them know, "Hey, if you're running this vulnerability as well, I got a notification from CISA letting me know that threat actors are leveraging this vulnerability. Maybe you should take a look at this as well." And we're seeing that more and more, the information sharing.

Again, that community defense approach. It's the only way we're going to get through this, because, otherwise, if we keep that information siloed and to ourselves, it's nice. We made one notification. But one is not even quite a drop in the bucket for the amount of vulnerabilities that are out there, so we have to do this in tandem with all the key players, with all the defenders out there.

Chris Riotta:

Yeah, I mean, when it comes to some of these specific critical infrastructure sectors like water and wastewater, I honestly don't know how you get much sleep at night. Just hearing about some of these cases, like in Florida a couple years back, where I believe it was a ransomware group that tried to hack into a local water operator and owner, and I think it was stopped sort of at the last second before they raised those levels, these kind of poisonous levels to some crazy degree.

I guess, can you tell me a little bit about how that work has actually happened with some of these smaller entities and organizations across the country that, as you mentioned, don't really have the resources to invest in cybersecurity and preventing these attacks? How is CISA getting to them and sort of helping them bolster their defenses?

Gabriel Davis:

Well, I have to say that it cannot be done without different parts of the agency. So in the cybersecurity division, we're out there identifying vulnerabilities, devices, systems that we know threat actors like to leverage, but the work is... That's only half the work. The other part of the work is actually getting out there, getting on the ground, making contact with those organizations. That's done in the integrated operations division, and that's at the regional level.

So CISA's broken up into 10 geographic regions, and we have to empower them to go out with that information, make relationships, and ensure that the message is getting out. And that's also being done through the ISACs. That's also being done through our industry partners. We're going full court press on getting the word out, also making individual notifications. But, hey, we have to keep passing this along. We have to make individuals and organizations aware. We have to keep them engaged.

Otherwise, where do we start? It becomes an insurmountable problem. You have to start somewhere. What we're trying to do is we're trying to prioritize, provide some guidance on where to start, and give some actionable tips on how to do that. Every organization's going to approach it differently. There's no one way to fix this problem. What we're trying to do is we're trying to give a series of tools where organizations can just make themselves a little bit better.

One of those key tools is the Cyber Performance Goals that CISA recently published. That gives an organization that just doesn't know where to start a baseline on how to secure themselves in this world. So there's multiple steps to it. There's a lot of different nuances, but ultimately it's about teaching the organization to defend themselves in such a way that fits their budget, that fits their priorities, and does not take down production.

We know we can't go water by water district and say, "Hey, you got to turn off water so we can replace these devices." Never will happen. We can't turn off the electricity to do these things. So we have to empower them in such a way that we're maintaining productivity, but also building in security as well. Because the infrastructure exists. Now we have to defend it.

Chris Riotta:

Right, exactly. And do you feel to that extent that the federal government and that you, and your partners, and your partner agencies who are working to provide this guidance and these sort of actionable items for these critical infrastructure owners and operators, do you feel that your teams have the resources, and kind of the funding, and sort of the wind beneath your sales as well? I know funding is obviously a huge challenge across government.

Gabriel Davis:

So it's always going to come down to having that community approach. There's never going to be one team that'll be able to take this on alone. Even if we got every resource known to us, it has to be done at the bottom-up level. What I usually like to tell folks is, I've got a 10,000-foot view. I'm looking down, and I can see some things that boil up, but I don't see what's at the ground level. So if you're at the ground level, you can tell me. You can better inform the government on how things are being done.

And that's where those regional personnel come in. That's where those state and local governments come in. That's where the private industry partners come in, so you can help steer the conversation as well. It can't be done, it just can't be done from a throw more money at it problem. We've seen that. That just is not something that's going to work for this type of disparate problem that's just everywhere.

Every day something gets another IP address. I'm sure someone here has a refrigerator with an IP address, a microwave. Everything's got an IP address now. Everything is being connected to the network. All those things present more attack surface, and we all have to approach this problem together.

Chris Riotta:

Yeah. Speaking of kind of expanding the attack surface, we have a question from Keith Nelson in the chat asking if cyber attacks increased during the shift to work from home status. I guess bringing it, tying it into critical infrastructure, can you maybe talk a little bit about how the sort of expanded surface level of space now that owners, and operators, and employees are working from wherever in the world now, how that has impacted vulnerabilities in regards to critical infrastructure?

Gabriel Davis:

Well, I'll let you know right now that just year over year attacks have increased. That's due to a number of factors. As stated, the increasing number of attack surface, just more and more devices are coming online being used remotely. So that's just inherent. I can't say definitively that the pandemic increased that number, because we've just seen it year over year. It's just something that has not decreased over time.

Also, a lot of these devices that are being used that in the operational technology side, PLCs and things of that nature, they were never designed for security in mind. Some of these protocols were just designed to work, and that's what they do. They provide productivity, and their lifespans are very different than IT lifespan. PLC's designed to last for decades. Your laptop is probably designed to last for about five years, max. So the life cycles are different, but the convergence, the cyber/physical convergence is happening, and we have to find ways to do this without taking down one side of the puzzle. So, I don't know if it answers your question. If it answers your question, awesome. If it did not answer your questions, please let me know, and I can add some more clarity.

Chris Riotta:

No, no, I think it did. I kind of assumed, unfortunately, that attacks have been just on the rise year after year, and so it kind of ties back to why CISA and your team are taking these sort of proactive measures. What I'm really interested in asking you, though, a little bit about is how do you measure progress when it comes to taking a proactive stance against ransomware attacks and attacks on critical infrastructure when obviously success would be then that attacks are prevented? So how are you thinking about measuring that? Is that something that your teams are kind of considering as well?

Gabriel Davis:

A hundred percent, right? That's the hardest thing is how do you measure something that didn't happen? And that's a challenge. So typically what we do is we'll look at historic data of things of similar type, similar size, similar sector, and we'll say, "Hey, this is an attack that was potentially prevented that occurred in this organization historically." So if we just look at previous attacks and look at the costs associated... Of course, it's not a one-to-one match, but it gives a good ballpark on the type of security and prevention that was provided there.

But also what I like to share is some of these things are inherently a part of our daily lives, like water. Water is just one of those things that it's very difficult to quantify if we get to the far end of that spectrum of how disastrous that could be when water gets contaminated. So that's one of those things where we say, yeah, we prevented an attack. We saved this amount of money, but also there were no casualties. There were no increase in illnesses. We didn't have to take a hospital offline.

Things like that, because all of it is coming together. There are multiple cross-sector dependencies that exist there. If you take down one, it has a trickle-down effect, and we saw this when the supply chain was interrupted during the pandemic, that if you take one pillar out, it could potentially lead to some long-term damaging effects.

So, yes, difficult to quantify in exact terms, but we don't attempt to do that. What we're attempting to do is we're saying, "Hey, we prevented this attack. There was an attack like this in the past. This is what it costs." But also what success looks like is an organization responds and says, "Thank you. We took that offline." We go back and make a double-check. We say, "You're good." That organization is now secure.

That's the win for us every time that happens. If it's a school, a K-12 school in middle America, or if it's somewhere on the coast, one of our territories out in the Virgin Islands, all of it is a win as long as it has a positive, we get a positive response, and we have accurate and demonstrable risk reduction, and seeing that exposure go down is that risk reduction.

Chris Riotta:

Yeah, that makes a lot of sense. Another thing that is sort of hard to measure is kind of the culture shift around cybersecurity, and particularly just like you said, the COVID-19 pandemic and the supply chain issues that happened throughout, I think maybe woke up some folks who don't particularly discuss and work in cybersecurity the way that we do every day.

I'm wondering, have you seen on the ground and in your work, in your collaborative work with these kind of organizations like schools and hospitals that may not have the sort of funding to be fully invested in cybersecurity, do you see that there is that culture shift taking place and that they're really seeing the importance of this work now?

Gabriel Davis:

Absolutely. It's all about the relationships, right? It's about letting those organizations know, "This is what we see. This is what we're encountering. We understand that your resource-constrained. Let us help you." And a way that we do that is through some of our services, one of them chiefly being the Cyber Hygiene Vulnerabilities Scanning service. That's a no-cost service that we offer to organizations throughout the country where we proactively scan for these vulnerabilities that we're looking for out in the open as well.

So that's just an extra layer of protection for these organizations. Again, I'm just going to keep beating this drum, right? There's just no one right way to do this, but I can guarantee you that we can't do it if we don't all work together, and it's got to be top to bottom, it's got to be culture shift, and it's all about passing that information back and forth.

Chris Riotta:

Yeah, and we've talked a lot about some of the tools and kind of the, maybe, I don't know if the word would be repositories, but a lot of the information that CISA has been putting out in recent years to kind of tackle everything from ransomware attacks to just known vulnerabilities. I think we have a question in the chat asking just a little bit more about where those are located. Could you plug maybe some of your favorite CISA accessible tools and initiatives? I know one of mine is the Shields Up campaign, but if you have anything that you would specifically like to highlight for our audience, I think that would be helpful.

Gabriel Davis:

Absolutely. So one of the key things that I look at almost every day are the ICS-Cert advisories. So CISA regularly puts out these advisories that are related to OT environment, and what it does is it does all of the background research. It tells you where these are commonly located. It gives you all of the vulnerability information. It tells you the device manufacturer. That's where I like to go, and that's something that's done inside of CISA as well. We're putting out these advisories, letting folks know that these devices themselves are vulnerable.

Also, as stated, the Known Exploited Vulnerabilities Catalog constantly being updated whenever there's information that can demonstrably express that something is being actively exploited in the wild and that there's a patch for it. So we're not just saying, "Here's a problem. Good luck." Everything that's being put out, we're saying, "Here's the problem. Here's the best way to fix it. Also, here's some best practices to go along with that."

Chris Riotta:

And just as a sort of final question for you, I'm just curious what you think the possibilities for the future might be around vulnerability warning. In a perfect world, how would you see organizations and entities across the public and private sector sort of working together to report these issues and mitigate them before they cause real damage?

Gabriel Davis:

In my perfect world scenario, I'm out of a job because we start seeing a shift to secure by design, right? Secure out of the box. That is where I start. That's where I see us going, where we're not... That is the exception, is seeing vulnerabilities in the open, but primarily we're seeing things being manufactured that are secure, that threat actors have to try very difficultly to get into. That's where I want us to get to. It's where you don't have to spend time and effort securing the device because it's already secure when you get it.

Chris Riotta:

Yeah, I think we could have a whole other hour-long conversation on the shift in accountability and the national cyber strategy, which we didn't even get to, but, unfortunately, we've run out of time. We have to leave it there. But, Gabriel, thank you so much for sharing your expertise with us and your insights. This has been incredibly informative.

Gabriel Davis:

Really appreciate you having me. I just want to get the word out. I want folks to feel empowered. I want them to know CISA is here as a resource. We're always willing to help. We want to drive down risk. That's our priority is demonstrable risk reduction in the nation.

Chris Riotta:

Absolutely. Well, greatly appreciate you being here. With that, I will turn it over to Justin Robinson, CTO of Cybersecurity Solutions with ThunderCat Technology for our next session. For FCW, I'm Chris Riotta.