Sean Gallagher:

Hi, I'm Sean Gallagher. I'm the information security editor emeritus of Ars Technica and a senior threat researcher at Sophos. Today, we are going to be speaking with Lesley Carhart. Lesley Carhart is the director of Incident Response at Dragos, and she's a veteran incident responder in the ICS space. That's industrial control system space. And I am pleased to have her with us today. Known as Hacks4Pancakes on Twitter, Lesley has some really deep insight into what goes on in parts of the internet we don't think about, the industrial control systems and other critical infrastructure that's internet connected or otherwise. Thanks for being here, Lesley.

Lesley Carhart:

Thank you so much for having me.

Sean Gallagher:

So, not much has been going on lately. I wanted to get your take on what has transpired since February and what that sort of means to critical infrastructure worldwide, what we've been seeing as far as how threats have changed because of the tensions and the ongoing war in Ukraine, other than war that's been carried on around that conflict. And we really want to drill down on what that means to not just companies, but everyday people, what the impact's going to be on people.

Lesley Carhart:

Yeah, so unfortunately, some of these things aren't new to those of us who are in the space. Sabotage and espionage, information in general, have always been a part of warfare. And something that we've noticed for years in the industrial cybersecurity space is that people from all different organizations, both military and terrorists around the world, have been pre-positioning to do things like sabotage and espionage via computers for years. The problem with that is, things like espionage and pre-positioning for future sabotage, they aren't flashy. They don't necessarily make the news. And even though researchers and security professionals, especially those working in industrial cybersecurity, have been aware of these things, they don't build budgets. They don't get people in executive and leadership positions for the most part to invest more in preventing these things from happening. So what we've had is a situation for years now where these more resourced organizations have been trying to build their capacity to when a geopolitical situation arose that it would be fruitful for them to do so to be able to attack infrastructure systems using computers, using cyber.

Sean Gallagher:

So I know that your boss, Rob Lee, recently did a presentation at an industry conference about one of the more recent discoveries in that space tied to a Russian threat actor. Can you talk a little bit about that particular threat and how it drilled down into those targets as part of that sort of strategy?

Lesley Carhart:

First of all, note that Dragos doesn't ever attribute activity to state actors.

Sean Gallagher:

Right. Understood.

Lesley Carhart:

We attribute to groups of hackers, criminals, et cetera, who are doing activity by their methods and their means, the way that they do things. We do that for a reason, because unless you are tied to state style intelligence organizations, it really is very difficult to be certain enough. And for a lot of reasons, it's not necessary for civilian organizations, for companies to know what country is potentially attacking them because the cost of being wrong is huge potentially. Also, there's negative connotations tied to that in terms of business. You might make an incorrect decision about where to do business or what employees terminate based on that. So that's not something we really do.

Lesley Carhart:

Now, something interesting that we have recently released information on is Pipedream, which was a collection of tools that could be used to potentially intrude into industrial control systems and cause and impact to certain types of systems. The fortunate thing is that this toolkit was caught before it was used to do something nefarious. However, that just adds to the knowledge that people are pre-positioning to do things in the future. They have learned over years, and certainly over the last couple of months, that sabotage, espionage, and information operations can be incredibly valuable as an element to traditional warfare. So it can be used to demoralize your enemies, it can be used to sow confusion and dissent, and it can also be used to impact the critical services that a civilian population uses while they're also dealing with a armed conflict.

Sean Gallagher:

So how much different are these types of threats from cyber criminal threats, where people are coming in and using things like a ransomware to the same sort of effect, disrupting manufacturing environments and things like that. I know there have been a number of ransomware incidents that affected operational technology. Is there any real difference in the impact? Or is it purely just intent?

Lesley Carhart:

You're talking about, in some cases, a hammer versus a scalpel. Your ransomware impact to industrial systems can be quite severe because ransomware tends to impact the systems that, say, industrial operators use for control of systems and monitoring systems. So having ransomware on those systems can impact their ability to safely operate them. We get to conditions where operators oftentimes have to shut down themselves because they can no longer be certain that their industrial systems can function safely or that they're doing what they're supposed to do. So that's certainly very, very impactful. However, it's not the same as somebody doing a very targeted technical intrusion where they say, try to poison the water or shut off electricity to a certain segment of the population. Those attacks are relatively hard and technical to conduct. They involve understanding the process and understanding the computer systems involved, the low level devices, like the control devices, and putting that all together in an intelligent way. They also have to understand the safety controls and the mitigations that prevent bad things from happening in those processes.

Lesley Carhart:

So what you end up with there is a situation where adversaries who want to do a very specific scalpel-like targeted thing as part of a greater effort typically, they have to have done a lot of reconnaissance and they have to have a lot of specialization and expertise on their team to do those intrusions. So that's why in the past, we've typically seen that from state sponsored type groups, more well-resourced adversaries. But now that ransomware commodity, malware authors, et cetera, are becoming more well resourced and more established, it's not outside the realm of possibility to expect them to start building those capabilities as well, if financially viable and interesting to them to do so.

Sean Gallagher:

How well positioned are we to protect against these sorts of attacks now? Did we learn anything from the attacks, say, on Ukraine's power grid over the past few years, leading up to the conflict that's going on now?

Lesley Carhart:

There's a lot more going on than the general population knows in these environments with people trying to defend industrial networks, improve the security of industrial devices, and prepare for potential worst-case scenarios. There is a lot of that going on. A lot of people in the space are really thinking about these possibilities, and they're deeply concerned. That said, some industries are much more well resourced than others. They're not created equal in the United States. A lot of our utilities are municipal. Some of them are large corporations that have a ton of cybersecurity resources. Conversely, the municipal ones might have one IT person working for them. So the ability to adapt and change security practices can vary vastly between city or town, or type of utility. And that's something that we're looking at closely, and organizations like CSA are looking at as well, to try to provide more resources to those less resourced but very, very critical utilities.

Sean Gallagher:

It sounds similar to some of the things I've seen going on in state and local government in general systems, in terms of the types of IT support they have in place to protect themselves. And we see it across small and medium businesses as well. They don't have the resources to deal with everyday cybercrime issues. Do you think that CSA is going be well resourced enough to help out organizations like that to get them better protected? And what else do we need to do to help them?

Lesley Carhart:

I can't tell the future. I think that they're certainly making valiant efforts to do so. The problem is huge, and the problem involves not just the US government, but our partners, our peers, industry partners, other countries. And things like take down efforts of adversaries, like criminal adversaries, usually are multinational efforts. So it really depends on how people pull together and what resources we're willing as a society to commit to defending this infrastructure. And like I said, there's a lot of things that are intangible in this space, and it's sometimes hard to get budgets and resources to defend things when an attack hasn't occurred yet. That's just the nature of doing cybersecurity or any type of security, any type of defense. So we will see. I'm hopeful, and I think that there's a lot of great people on multiple fronts, including CSA who are really pioneering and fighting for the resources that are needed.

Sean Gallagher:

Can you talk a little bit about the difference between the operational tech, the industrial control system tech that's out there now; and what people deal with, sort of the everyday IT, they deal with, in terms of how quickly it changes; and what kind of vulnerabilities happened there rather than on your desktop or your server?

Lesley Carhart:

Sure. So one of the major differences is the long life cycles of this stuff. When you go out and you say buy equipment for a power generation facility, you're buying things as a package. So you're buying in layers of systems that work together to generate power, including computer systems and control devices, and they're all certified and tested and warrantied to work together. You can't just suddenly walk in there like you might do in your enterprise IT environment and decide to upgrade everything to a new version of Windows. That could cause an impact to the way the system functions, it could make things operate unsafely, and it can certainly also do something like void your support contract for that equipment.

Lesley Carhart:

So really, some of these organizations are stuck with the same systems for 10, 20 years with only upgrades that are approved by the vendor. And that's by design because the number one thing that these systems have to do is function, function efficiently, quickly and reliably so that they are providing safe control of whatever they're doing, whether that's generating power, or getting water out of pipes, or making widgets in a manufacturing facility.

Lesley Carhart:

The number one thing, again, is not cybersecurity or encryption or having the newest computer, it's things functioning properly. I mean, think about the ISS running on its ancient computers in space. They do that because it works, and it's reliable and it's trustworthy. The scenario that they're in is incredibly, potentially dangerous. That's what we're dealing with industrial, so we have to be really creative. We have to think outside the box to do cybersecurity there because it's not as simple as going through the checklist and updating your operating systems and maybe installing modern security tools. All of those could potentially have a unexpected and very negative impact on what the process is doing.

Sean Gallagher:

You talked a little bit about the kinds of things that people might try to do with hacking into ICS systems, that's redundant, into ICS. If you could throw a switch, what one thing would you change about how people are deploying ICS today that might make the greatest reduction in the level of risk associated with them now.

Lesley Carhart:

Start with the fundamentals. Understand your environment. Have good network maps. Have good asset inventories. Understand how your systems are connected to one another and how they might potentially be connected to the internet, and vet that routinely. If you don't start with the fundamentals and understand what you're securing, it's incredibly difficult to do more complex things in cybersecurity. So start with those. I oftentimes have to go into environments to do incident response where nobody knows what's out there, nobody knows what systems are in play or what operating system is in use. They don't know if there's internet connections. They don't know what other remote access sectors there are into the network. And that makes my job as an investigator, who's trying to get things back up and running, very, very difficult.

Lesley Carhart:

So we could jump ahead to more complex security tools and things that are flashy and new in an enterprise cybersecurity space, but what I really need in the industrial space as a cybersecurity professional is just the fundamentals to be put in place. So start with understanding the environment, then building in things like segmentation and basic security practices where possible. That's where people need to start. Another thing that everybody who's watching this needs to understand is that these industrial systems are everywhere. They're all over the place. They are your building control networks, building automation, the things that provide backup batteries for your data center, your infrastructure for cooling your building, which could potentially be incredibly impactful to your operation. So they're all around us. They're not just in these very specific industrial environments you might be thinking about, and they can have huge impacts on operations.

Sean Gallagher:

Right. That sort of gets into the question of what people can expect as a personal impact to some of these things. You talked about cooling systems and things like that. I mean, could someone theoretically take control of a system on an HVAC environment or some other system in an office space and make it not just unpleasant, but hazardous to be there?

Lesley Carhart:

Absolutely, and hazardous to equipment, especially. So consider what happens to your data center if, say, the fire suppression system is triggered, or it overheats because it's hot outside and your air conditioners no longer work. That's not something you probably think about frequently because you're thinking about the data security of the servers in your data center. But think about what that actually could do to the equipment over hours or days, depending on conditions. So I've seen incidents where things like that that are tangential support systems have had huge impacts on an operation because people didn't think about that potential outcome. And what I really encourage there is doing some consequence modeling, so thinking about what's your worst day ever in your operations. And that can really vary, it depends on your mission as an organization. So think about that, consider that, and then start working down to potential scenarios where that thing could occur and what systems could cause that condition to happen. So start working down to broad systems and then very specific ones, and that'll give you an idea of where you really need to focus your cybersecurity efforts.

Sean Gallagher:

Do you think that the movement of a lot of systems to cloud back ends and things like putting edge computing connected to ICS that tied to cloud? Does that make cloud the Achilles' heel in some cases? I mean, if I could target the cooling at a data center for, say, Amazon and shut down cooling in AWS in Virginia, that could be a pretty big economic impact across a number of industries.

Lesley Carhart:

Yes and no. I would say that for a large, maybe the vast majority of organizations, Amazon or Microsoft, or those big data center providers, the well-known ones, probably have a better business continuity plan in place and possibly a larger and better resource cybersecurity program in place. So cloud is not inherently worse or better for cybersecurity. It's just different. You're just moving your risk, moving your cybersecurity concerns somewhere else. And the same types of cybersecurity concerns still exist, but it really depends on your capacity to do cybersecurity of, say, your data center and the system's in it versus handing that risk off to a third-party organization with the level of confidence that they give you and the level of legal and technical assurances they give you. So that's a decision that every organization needs to make for themselves.

Sean Gallagher:

So looking at the slow pace of change in ICS and the vulnerabilities that persist for so long, do you see any particular evolution of how the companies that provide industrial control systems to customers are going to change their technology to make it simpler to secure? Or is that something that's so long off in the future because of the cycle of ICS that we're not going to see it anytime soon?

Lesley Carhart:

We are starting to see improvements to cybersecurity and industrial devices and industrial networks. It just depends on the age of the system. As we're seeing major version updates, we're starting to see Windows 10, which is a major improvement deployed in industrial systems. Of course, that means it'll probably be seeing Windows 10 for another 30 years in those environments. But right now we are starting to see improvements. We're starting to see more security suites be sold as part of industrial deployments, also incident response retainers are a big focus from a lot of the vendors right now. So if you do have an intrusion, you have an incident response expert on call who you can contact.

Lesley Carhart:

So we're seeing a lot of that. There are really efforts to make cybersecurity better holistically for industrial systems. However, that might not look like what it looks like in more familiar enterprise networks. Like I said previously, you can't necessarily just tack on cybersecurity elements like EDR to these industrial devices. It's just not feasible because it adds overhead and potential risk. However, adding things like ability to add security suites to monitor passively, add incident response capabilities, we absolutely are seeing that happen. And that's very positive in terms of direction.

Sean Gallagher:

Okay. I know you've worked a lot of incidents, and you can't talk about most of them, but can you talk about sort of the prevalence of what you're seeing in terms of current threats to ICS? I mean, we talk about the cyber war stuff, and that obviously hasn't happened much outside of a very specific set of environments. What day-to-day are you seeing as far as what you have to respond to in these environments, when there's an incident? What are people facing daily right now?

Lesley Carhart:

Yeah, so we just released a year-end review report for last year where we talk about a lot of the incident types that we've seen by numbers, but I can give you a quick overview of the three types of things that I'm responding to typically and my team is responding to typically. The first one is the commodity malware types things, so ransomware, et cetera, which, as I mentioned previously, can be very impactful to an industrial environment because it's disrupting control and ability to see what's going on in the process. Again, that can kind of create those situations where things have to be shut down.

Lesley Carhart:

The second thing that we respond to is insider attacks, and those can be purposeful or not purposeful. So the purposeful ones, of course, are somebody's getting fired or separated, they're upset and they break something. And the people who monitor and manage those industrial systems every day are generally very trustworthy, but of course there's always exceptions, it's human nature. They know how to break things. They have that knowledge of how to take the system down and how to do the most damage to it, so it can be very disruptive. But there's also the people who don't mean to cause a cybersecurity incident at all, and they're totally honest people. But they, say, want to watch television at work so they plug in a USB drive with their shows on it, or an antenna to the computer or something, and they infect everything, and they don't mean to. Maybe they're doing service maintenance and they plug in a modem to the sensitive industrial network because that's how they think they need to do it. And that can still have a huge impact, even though it was totally unintentional.

Lesley Carhart:

And then the third category of things, of course, are those more sophisticated, advanced type adversaries. And those are the groups that are usually in it for the longing. They are conducting reconnaissance. They're doing things like exfiltrating screenshots of the system operating controls so that they can understand perhaps in the future when it's worthwhile to them how to conduct an attack.

Sean Gallagher:

So you've talked a little bit about what people can do to make things better. What is the sort of state you see in place right now in terms of the level of protection organizations you deal with have in place? I'm sure it varies widely. Is there any particular area where these organizations fall flat on a regular basis besides staffing? Because it sounds like it's a big one.

Lesley Carhart:

Staffing is a huge one in resources in general for every cybersecurity organization, but here's some advice that I can give people. The Department of Energy in the United States has a tool called C2M2, it's a cybersecurity maturity model assessment. And what that is, is a survey you can take yourself, it's a self-survey, for your capacity to do cybersecurity in, say, your industrial environments. It's pretty straightforward. It's just simple questions that you answer, and you rate yourself on a scale of how mature you think you are in your capacity to do various things. Ultimately, what you get is, they've got three maturity levels, one, two and three.

Lesley Carhart:

The first one is, I know how to do the fundamentals. Okay if you're cybersecurity in this space. The second one is more intermediate. So you've moved on, you've done the fundamentals, and now you're adding in things, like more security tools, monitoring capacity, et cetera. So you're a little bit more mature. And the third one is your very, very advanced, very mature, very sophisticated cybersecurity capacity. So if you go out there and you do that survey, you'll kind of understand where you stand next to other organizations in terms of your ability to do various realms of cybersecurity from incident response to authentication, et cetera. I really recommend that. It's not a difficult process. It's a little time consuming. It can take a couple days perhaps to get the bright people in the room and do the survey.

Lesley Carhart:

But what you want to do there is build the fundamentals out first. So start with maturity level one. You want to finish everything there before you move on to the next maturity level. I see organizations across the spectrum in terms of maturity, but the biggest problem that I see is when they try to jump ahead. So they haven't finished the fundamentals, they haven't finished this first maturity level, and they're jumping ahead to really sophisticated stuff that isn't going to provide a lot of value because they don't have basic things like an incident response plan or the ability to document and understand their network, have an asset inventory, et cetera. So if you want to understand where your organization, your facilities stand in context, I recommend that you go out to the Department of Energy website and download their toolkit for C2M2 and give it a shot in your organization. It's worth the time, and it'll help you understand where you stand.

Sean Gallagher:

You sort of bring things that wrap things up a little bit. I want to talk to you about where the people come from to do this now. We talk about the cyber workforce, and there's been a lot of ranting over the past few years about the lack of a cyber workforce. Every time I look at an ad, they seem to be looking for somebody with 10 years of experience for a junior position. Where do we get the people to do this stuff? And what has to change about how we hire and develop people to secure the world we're in?

Lesley Carhart:

So there's a very limited pool of people who do industrial cybersecurity. And it's very, very critical that we have a good pipeline for it. Now, where do I hire people? Well, I certainly hire people out of the industrial space who are starting to learn cybersecurity because I can train them on cybersecurity, or vice versa. I can hire people out of the cyber security space who want to learn more about industrial. Those are things that can be trained. You do need to have fundamentals in those area, but you also need to have good critical thinking skills and not something I can't teach. So I'm always looking for people who can think outside the box because we have to think very, very creatively and learn about a lot of different processes and pieces of equipment and solve very interesting problems in industrial cybersecurity.

Lesley Carhart:

So number one thing, pipeline off the street is fundamental computer knowledge, but also that ability to think very, very creatively and think through problems, like how do we secure these very, very valuable high-risk systems without being able to use modern tools at all. And that's not necessarily something they teach in college. That's not something that you necessarily learn in generic cybersecurity certifications. You have to get to industrial specific things, and those are very limited. So it is incredibly important that we keep training people in industrial cybersecurity and that we get more people through a pipeline into those roles from other spaces, from either the IT side of things or from the industrial side of things, because there's just going to be more and more demand in this niche. It's a growing field, very rapidly growing field. sub, I probably know 90% of the people who work in my space in industrial and center response. It's very, very limited.

Sean Gallagher:

Are there any things that,, say the educational sector or people in the training space can do to help build the pipeline? You talk about things you can't learn in college right now. Certainly, most of the people I know who are in this industry did not get a degree in cyber, anything. How do you give people the tools to get them into the pipeline to begin with? Where does that have to happen?

Lesley Carhart:

In terms of education, focus on those critical thinking skills as part of a cybersecurity curriculum. So learning things rote has value in some fields of cybersecurity, but industrial cybersecurity, we really need people to be able to know how to learn. We need people to learn to learn. We need to teach them how to problem solve and think through complex situations. So that's a really important part of the curriculum. Also, understand that industrial cybersecurity is a huge space. There's a ton of different industrial verticals, and the equipment and the protocols and the problems are different in each one of them.

Lesley Carhart:

So if this is something that you want to teach or you want to learn, try to focus on an area to start out with, focus on a technology or a vertical in the industry, and that's going to help you a lot. It'll serve you well.However, just focusing on industrial as part of cybersecurity in general would be very valuable in college curriculums and technical training curriculums. Take the time to at least provide some lectures on the topic. There's a lot of folks who are in this space who are very interested in sharing their knowledge. Have them come talk to your students. Have them learn a little bit about the space so that they can see if it's something they're interested in doing.

Sean Gallagher:

Do you feel like people are getting enough exposure to ICS hands-on at all in those environments? Or do things like ICS Village, are those scalable in terms of getting things out into communities that might be interested in that?

Lesley Carhart:

Yeah, ICS Village is an amazing community project to educate people on how industrial cyber attacks and cyber defense work. They're doing incredible work at a lot of different conferences around the United States. And I can't say enough good things about them. We can certainly use more efforts like that. And I'm sure that they always can use more volunteers and more support for their organization. So, any organization that's teaching about industrial cybersecurity right now is incredibly valuable because, again, such a limited pool of people and such limited training on the topic is available.

Sean Gallagher:

Any parting comments on this? I know I've asked you a lot of questions. Anything you want to share that I haven't asked about?

Lesley Carhart:

Take the time to go see if there is industrial technology in your environment. You'll probably be surprised. And then next, consider what you do if there was a compromise of it. Do you have some kind of plan in place? It's not going to be your generic incident response plan for your enterprise organization. You need to think about these things discreetly because they are totally different can of worm. Take a day or so to really do that vetting in your environment, and consider the impacts and consequences that an industrial intrusion could have to you. A lot of organizations aren't doing this until something goes catastrophic later on.

Sean Gallagher:

Thank you so much for your time, Lesley Carhart. I appreciate you taking time out of your extremely busy schedule to talk with me today. Good luck on all of the travel you have ahead of you next few weeks, months. Again, thanks for joining us.

Lesley Carhart:

It was an absolute pleasure. Thank you for having me.

Sean Gallagher:

For those of you who could join us today, thank you for joining us. If you are going to be in the DC area on May 12th, we will be having a live event, Ars frontiers, at which I will be moderating two panels, which I'm super excited about. Got some great people lined up to talk about privacy and security. There are limited tickets available still for the live events on May 12th. It will also be streamed online. And I hope that you can join us either in person or through your screen.