UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

34TH REGULATORY INFORMATION CONFERENCE (RIC)

+ + + + +

TECHNICAL SESSION - W17

EMERGING CYBER THREATS TO INDUSTRIAL CONTROL SYSTEMS

+ + + + +

WEDNESDAY,

MARCH 9, 2022

+ + + + +

The Technical Session met via Video-Teleconference, at 3:00 p.m. EST, Jim Beardsley, Chief, Cybersecurity Branch, Division of Physical and Cybersecurity Policy, Office of Nuclear Security and Incident Response, presiding.

PRESENT:

JIM BEARDSLEY, Chief, Cybersecurity Branch, Division of Physical and Cybersecurity Policy, NSIR/NRC

ROBERT ANDERSON, Nuclear Cybersecurity Consultant, Idaho National Laboratory

JACOB BENJAMIN, Director of Professional Services, Dragos, Inc.

MARK BRISTOW, Chief, Cyber Defense Coordination Branch, Threat Hunting Division, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security

JOEL MAX, Industrial Control Systems Lead, Federal Bureau of Investigation

TAMMIE RIVERA, Cybersecurity Specialist, Division of Physical and Cybersecurity Policy, NSIR/NRC

P R O C E E D I N G S

3:00 p.m.

MR. BEARDSLEY: Welcome, ladies and gentlemen. We're glad you have joined us for this year's Cybersecurity RIC session. I'm Jim Beardsley, the Acting Deputy Director of the Division of Physical and Cybersecurity Policy in the NRC's Office of Nuclear Security and Incident Response.

We're very excited about this year's session focused on the emerging threats to industrial control systems. This topic is very relevant to the current state of cyber security in virtually every industry including nuclear power.

Before we get started, I want to make a couple comments about the NRC's Cybersecurity Oversight Program. In 2021, the staff completed the inspections of nuclear power industries' cybersecurity program full implementation. The staff found with reasonable assurance that industry understands the cybersecurity regulatory requirements and has implemented their cybersecurity plans.

Also in 2021, the staff developed a new cybersecurity inspection program that will focus on

industry's ongoing implementation of their cybersecurity programs. Each licensee will be inspected every two years and those inspections started last month.

The staff have developed a revision to our cybersecurity regulatory guide and it's available for public comment. The revision is designated as Draft Guide 5061 and can be found in the NRC's public document repository, the Agency-wide Documents Access Management System or ADAMS.

Now on to the session. We have a fantastic line up of speakers covering diverse perspectives on the subject of cybersecurity threats on industrial control systems. I'll introduce the panel members before we get started. There are more detailed bios for each of them available through the RIC-2022 platform. If you have questions for the panelists during the session, please enter them into the RIC platform using the Q and A tab and if you have a specific panel member you wish to address the question, please note that in your entry.

Our first speaker will be Jacob Benjamin. Jacob is the Director of Professional Services at Dragos, Incorporated.

Second, we will have Joel Max. Joel is the Industrial Control Systems Lead at the Federal Bureau of Investigation Cybersecurity Division.

Our third speaker will be Bob Anderson. Bob is a nuclear security consultant at the Department of Energy's Idaho National Lab.

Finally, we have Mark Bristow. Mark is the Branch Chief for Cyber Defense and Coordination in the Threat Hunting Division of the Department of Homeland Security Cybersecurity and Infrastructure Security Agency. Mark may or may not be able to join us. We're still waiting for him to arrive. If he does not, we'll move right to Q and A after the first three speakers.

MR. BRISTOW: Hey, Jim, I'm here.

MR. BEARDSLEY: Mark is here.

MR. BRISTOW: Sorry, I had some tech issues. Sorry about that.

MR. BEARDSLEY: Mark will be the fourth of our speakers and so we'll kick it off with Jacob. Jacob, go ahead.

DR. BENJAMIN: Thanks. I was looking for --- are the slides up?

MR. BEARDSLEY: Yes, you're good to go.

DR. BENJAMIN: I don't see the slides, but that's okay. So I wanted to talk to emerging ICS threats and the first thing to do is to talk about threat groups. So Dragos collects and analyzes information on cyber intrusions and attempts to compromise ICS networks. We create profiles of known groups targeting ICS environments so we can focus on how they operate. Then we establish robust analytics with comprehensive data around their actions, their capabilities, and their intentions.

Currently, we track 18 ICS threat activity groups, two of which have shown interest in or targeted nuclear. So if you'll skip ahead, I think two slides, you'll catch up to me. Perfect. Thank you.

So as I said, we're going to highlight two groups here and these two are the ones that are known to have shown interest or specifically targeted nuclear. The first one, Wassonite, so in October 2019, Dragos identified the adversary Wassonite targeting the Kudankulam Nuclear Power Plant in India. Later, intelligence research, combined with public announcements from that plant, confirmed that the adversaries had breached their IT network.

Dragos also identified a pattern of activity associated with the same tactics, tools, and techniques spanning across multiple ICS entities that also included electric generation, nuclear energy, manufacturing, and space-centric research.

So we also have Dymalloy, Dymalloy operations include deep ICS environment information gathering, operator credentials, industrial process details using tools like Goodor, DorShel, Mimikatz.

Dymalloy targets geography-wise Turkey, Europe, and the United States. It has links to other intel -- so other companies that track intel, right? So Dymalloy is linked to Dragonfly 2.0 or Berserk Bear. So Dymalloy successfully obtained HMI screen shots while conducting reconnaissance and target operational networks. And this was documented in a CIS alert in March 2018.

So Dymalloy's victimology includes U.S. electric generation and nuclear. As you can see here, we kind of have these trading card rep profiles here that kind of highlight their geography, their victimology, and some of their common TTPs.

So I've compared these two here and they share some TTPs that I wanted to highlight. So both

groups use spear phishing attachments to gain initial access and both groups leverage valid accounts to laterally move across the network. And both groups also use credential harvesting and privilege escalation and to do that, they leverage the tool Mimikatz.

So if you go to the next slide.

So we recently released our fifth annual year in review report on ITS cyber threats, vulnerabilities, assessments, and incident response observations. And here are some key findings from our proactive service engagement. So this data set includes engagements from many industrial infrastructure sectors, not limited to nuclear. So it has electric, oil and gas, food and agriculture, pharma, chemical, transportation. It's got a number of them.

So let me highlight here on visibility. So the greatest and most common recommendation that Dragos has is to increase visibility of the OT networks. So visibility is critical for network security and it facilitates the prioritization of future improvements.

Additionally, streamlining detection of

response capabilities is really only possible with an increased understanding of the network and its network components and that can only be done with visibility. So the specific numbers here that we're looking at, so 86 percent of our service customers here had limited or no visibility into their ICS environment. So poor security perimeters, external connections to ICS, and shared IT and OT credentials, those are common to the OT industry in general, but not to nuclear. So nuclear has, as you are well aware, has strong network security perimeters, hard breaks, and segmentation, but they do still suffer from poor visibility.

And I'll talk more about this in the next slide, so if you'll go ahead and go to that. One more time. Thanks, perfect.

So one of the questions I had when we were preparing this panel, they asked me to speak on why visibility was still needed even with the implementation of a data diode. And so a harsh truth is that prevention is ideal, but it's not guaranteed. And preventative countermeasures like segmentation they atrophy over time. And so things like spreadsheets, drawings, they become obsolete quickly

and they almost never resemble the true state of the network.

So visibility provides that site picture for how the processes and work flows are actually executed and leads to that understanding of normal in the OT environment and also leads to continuous validation that those preventative controls are working, that there isn't any bypasses of data diode.

And then so -- yes, so like I said, visibility leads to understanding normal in your OT environment. So knowing normal adds that valuable context to accelerate like the defender's situational awareness and things like change detection.

So I do want to highlight here a little bit like what do we consider limited visibility because it's easy to say what does that mean? So we considered a finding limited visibility if the asset owner was only monitoring the IT to OT boundary, if they had an incomplete or inaccurate asset inventory, or if they were doing limited or manual log collection, or they were monitoring OT communication but without OT protocol dissection. So without these items, defenders are blind to critical network trapping that's happening on the operational network.

So that leads me to like how do you get full visibility? What does that mean? So full visibility is achieved when networking device logs are centralized and can correlate various network segments with traffic analysis and active inventories. And so one thing key about visibility is without visibility most threat intelligence is unactionable. You can't do anything about it. You have this alert for this vulnerability, but you don't know if you have that asset or you don't if you have that asset in that configuration. So but threat intelligence itself is very necessary, right? So you need it to provide the context for when you do detect something to understand whether it's a false positive or to actually the most tricky situation is determining whether it's a process anomaly or a cyber-attack. And to do that, you need the context that comes from threat detection.

And so threat detection and visibility, they both lead into being able to early detect things with the appropriate context that allows a defendant to rapidly execute a playbook and selecting the correct playbook which will then expedite response, containment, and remediation efforts.

So overall, to kind of wrap it up in a sentence or two like why do you need visibility when you have a data diode? Well, visibility leads to early detection which leads to quicker recoveries, and ultimately minimizes your financial, operational, and even safety impacts. Thanks. So that's what I have for my slides, Jim.

MR. BEARDSLEY: Thanks, Mark. Why don't we go to Joel.

MR. MAX: Thank you. So today, I'm going to talk a little bit about how the FBI views a threat to the nuclear sector in the industry and then I'll talk most of my time about how do we engage with the FBI and answer any questions you may have on how to work through an incident both ahead of time and during an incident with the FBI.

So, kind of to level set, when we look at the threat landscape, China and Russia are the two that rise to the forefront which is to nobody's surprise, especially when you look at their ICS attack capabilities. They have a lot of resources to throw at that and I think that what we're seeing overall in the landscape is that there's more and more capability being developed around the world and

that the adversaries are looking to whole different sectors of infrastructure or risk to include the nuclear sector. And so when we've met with industry and talked about the threat, I think that's pretty straight forward.

Now when you look at what are these adversaries looking for, they go after a lot of stuff that's pretty easy to get in the open source especially things like social engineering, going on LinkedIn and finding out who works at what companies, the type of makes and models, the things that you may use in your OT networks. They look at -- they're looking for sensitive internal documents, things that can help them better understand their network, understand the physical layout of your facilities, you know, really looking at every aspect of how to find that one weak link. Because as we all know in cyber, it's so difficult to protect every part of the fence line so to speak.

And just like Benjamin was talking about with having visibility, the FBI's number one recommendation to industry is to have a good baseline. But you can't have a good baseline if you don't know what's in your -- what assets you have and

so understanding that baseline and having that set ahead of time is so critical because whether it's China or Russia or other actors, they're doing things, you know, like using legitimate credentials and the stuff that you just hear about, that's much harder to detect unless you have that baseline. You understand how traffic is moving in your network, what users are logged on, what does that look like specifically.

So really, we continue to recommend trying to get that baseline because so many of the other recommendations that come out of the government or ICS really aren't applicable to nuclear just because of the way the legacy system is and the way its architecture is, is just not the same as many other sectors.

And it's not as easy to go back and retroactively fix a lot of things which kind of leads me to the portion of working with the FBI. We really recommend that industry works ahead of time to identify not only in your continuity planning, but working through which office, which local FBI field office is nearest to you. Each of our 56 field offices have a cyber squad that's especially trained

to handle incident response to critical infrastructure. And I know Mark is now here to talk about what CISA does, but we work very closely with CISA to provide kind of that proactive engagement with industry so that way everything can be kind of discussed ahead of time so that you're having those conversations before the incident not after the incident has happened. The last thing you want to do is be in a situation like Colonial where you're trying to put the pieces together when the whole world is watching.

So if you can engage with the FBI early, talk about what your plans are and then that helps us figure out we can best help you and also give you a sense of what that looks like from an incident response, so when we come in to do things like evidence gathering, intelligence collection, and working with CISA who is doing a lot of the incident response, you know what that looks like. You know what the personnel is going to be from a legal perspective, it's always helpful to have general counsel engage early to look at those MOUs, what that might look like. So I think that is really a key level of -- a measure of success for entities that

we've seen who have been victimized. Those who have had a previous relationship with us have had a much smoother process. It just makes it a little easier on everybody.

So from that standpoint, the best way to connect with the FBI is at the local level. And so whether you're -- and that's not even just in the 56 field offices here in the United States. We have a number of offices overseas in our legal attache offices. So whether you have a presence here in the United States, you may have partners overseas or at other locations, you can get with the FBI almost anywhere in the world and as a part of that, we work hand in hand with CISA to figure out what that solution looks like for you, to move that intelligence from classified to unclassified channels when we came through things like private industry notification and flashes and joint cybersecurity advisors with CISA and NSA and others, and where they work in trying to get that intelligence we push that out to industry a bit more faster than what we have in the past.

So that's really kind of in a nutshell how the FBI views a threat and how we like to work

with industry ahead of an incident, hopefully, and if you do have that bad day and you're trying to work through that incident, we're happy to work with you through that as well and, hopefully, make that process as easy as possible, and ultimately from a law enforcement perspective, bring to justice those that are going after systems, that are going after people and your priority information. Those are the type of things that we're interested in doing.

So I think that's it for me. I'm happy to answer questions once we get to that point.

MR. BEARDSLEY: Thank you, Joel. And now we'll go on to Bob Anderson.

MR. ANDERSON: Great. Thank you, Mr. Chairman. If we pull up -- okay, we have the first slide up there.

I want to talk about a couple areas that I've been working on in the last several years that are kind of near and dear to me and that is cybersecurity for advanced reactors and cyber-informed engineering.

If we go to the next slide and we take a look at what the cybersecurity landscape might look like or the digital footprint with advanced reactors,

we know that there's going to be an extensive use of digital technology. We know that there's going to be new I&C smart sensors that are being developed. We assume that there will be some built-in diagnostics as part of that. This may bring some new protocols that we might have to worry about from a cybersecurity perspective.

We're expecting to see more wireless technology increasing. We know that field programmable data rays are being suggested for safety systems, especially within the small modular reactor and micro-reactor worlds.

And then, of course, with the extensive use of digital technology, we expect to see more frequent upgrades of software and firmware and patches. And what does that look like? What are the processes going to be like in place and how do we protect against the more frequent upgrades?

And then we also expect that there's going to be some ties, some sort, to smart grid, interactions with intermittent power, whether that be wind or solar or something like that which will probably produce a different type of operations.

And then we hear a lot about digital

twins. And oh, by the way, what does that even mean? I'm not even sure I know what that means today. I've heard a lot of different definitions of what that's supposed to be, what it's supposed to do. Maybe it's going to help us run some models and simulations to have more efficiencies or things like that, but again, we're hearing these words here in the industry right now.

When it comes to remote operations and remote communications, what's that going to look like? How do we protect those? Those may look a lot different when you have microreactors that maybe be far away from like a control room potentially or something like that. But we know that there's going to be autonomous operations that people would like to have to reduce the people footprint there. There might be some different type modes of operation including load following, AI, artificial intelligence, and machine learning.

I think one of the biggest concerns around that is what are the boundaries for use in the nuclear industry? What are those use cases for AI and ML? Like I would hope that we never really control with artificial intelligence. I would hate

to wake up the next day as an operator and find out that the AI learned something new overnight and has a new way to control. So these are some things that we need to be careful about from a cybersecurity perspective. Maybe there's some increased monitoring as well.

And in supply chains, I think we all understand that supply chain is huge right now. There's a lot of issues surrounding that, especially when you look at and there are some SMR vendors themselves, they are part of the supply chain. And they have a lot of sub-suppliers. And there are probably a lot of international systems and components that they get. And so it's really an international potential problem that we have to solve on the supply chain.

But then when you go to the next slide, how have the regulators really addressed this advanced reactor cybersecurity? Is it going to be -- is the guidance going to be prescriptive? Are we moving towards performance-based guidance?

I heard a lot in the last couple of days about risk-informed guidance and regulation. So what would be a hybrid of the two? What's that going to

look like in the end?

From the international perspective, what about harmonization of regulation? I know that vendors want to sell their products worldwide. Is there a way to talk to regulators from other countries to make sure that whatever regulation and guidance comes out now is harmonized in some form or other so that there's not a lot of rework potentially on the vendors themselves.

What about design basis threat updates? I would imagine with the high digital footprint that we may want to update our DVTs more often. We always see new techniques and tactics and procedures from the adversary. There's different capabilities and intents and motivations. What's that going to look like especially from like SMRs or microreactors?

And then we come down to a main topic with staffing qualifications. And not just competent authorities, but operators, too. And what's that going to look like from a cybersecurity perspective? How do we educate everybody in the nuclear industry about cybersecurity

And that really leads me into the second area that I want to talk about in the next slide and

that is cyber-informed engineering. This is an area that the Idaho National Laboratory and Department of Energy have been working on for several years. Jacob Benjamin, who used to work for the INL, was a contributor to this as well. But it's a cyber-by-design concept and this is really looking at cybersecurity as a foundational element of risk management, especially for functions supported by digital technology.

So what does that exactly mean? What that means is that we want to make sure that we reduce the risk from a cyber-attack, right? Can we mitigate it? Can we eliminate things? This whole concept is focused on engineers and technical support, so it's an engineering approach, not an information technology approach.

We were looking for opportunities where potentially we could engineer out some of the cyber risks and maybe through that process we've got some cost savings, but ultimately, we want to look for applying more effective security approaches. The last thing we want to do is wait until the design is completely done and then find out that we really can't bolt on any cybersecurity controls when we could have

done it earlier in the design phases.

And again, part of this concept is looking at the entire system engineering life cycle. If we can get small modular reactor and microreactor vendors looking at their conceptual stages from a cybersecurity perspective, then maybe there's some areas where the cybersecurity specialists can get involved and help direct some areas that may be less vulnerable to cyber-attack. And of course, we're really trying to stimulate an engineering culture here of security, similar to what we already have with safety.

And if you go to the next slide, in 2020, the National Defense Authorization Act directed the Department of Energy to develop a DOE national cyber informed engineering strategy. I was a part of the technical teach that helped put this together and it's really cybersecurity as a foundational element of risk management for functions aided by digital technology. And again, this is for the entire systems engineering life cycle.

And coming out of that strategy, we have five strategic pillars. One of them is awareness. So what is cyber-informed engineering? Who is it

for? What does it work? What conditions do we use it in? Et cetera, et cetera. It's really about getting the awareness of CIE out there to the community.

Number two is education. How do we educate the young people coming out of the universities? Can we get into the universities and help them provide some curriculum on cyber-informed engineering? And how do we educate, of course, the existing fleet of engineers that are out there within the energy world?

And then development, that's actually developing the products and the application for CIE. What are the tools that we're going to need? What are the processes and procedures that go along with this so somebody can take it and actually use it and not just have a conceptual idea in the sky there? So that's what the third one is about.

And then, of course, we take those tools and processes and we apply it to the current infrastructure, energy infrastructure, and not only to the current one, but also to the future R&D energy systems which small modular reactors and micro-reactors totally fit right into that slat. And so if

you want to know more information, we have a website on cyber-informed engineering that's currently hosted on the INL.

And if you want more information, if you go to the next slide, you can talk to Cherylene Caddy, who is the Senior Advisor for cybersecurity for DOE's CESER organization, or Cybersecurity Energy Secretary and Emergency Response Organization, or you can email myself and I will get you the answers one way or the other.

But those were the two main areas I wanted to talk about that I've been dealing with a lot recently. I also work with the International Atomic Energy Agency a lot. I just got back a couple of weeks ago on a technical meeting on small modular reactors and micro-reactors and there was a lot of great information that came out of that that hopefully the Agency can help answer for a lot of the member states.

And with that, I'll give it back to Mr. Chairman.

MR. BEARDSLEY: Thanks, Bob. And now to hit clean up, how about Mark Bristow.

MR. BRISTOW: My favorite spot in the

line up to include right before lunch. Those are always the best times.

So thank you and apologies for my technical difficulties to get us going. But just a couple of things I want to hit on because I think -- I really want to leave some time for Q&A and quite frankly, my colleagues here on the panel have really hit a lot of some of the same points I want to make, but I want to touch on a few things.

So the first thing I want to touch on is so -- hi, I'm Mark Bristow. Sorry, I didn't introduce myself the second time. I'm the Branch Chief of Cyber Defense Coordination in CISA and I want to talk about three things in particular. The first one is if you're not familiar with CISA just and like working with us, kind of what threat hunting's role is here, and similar to what Joel was talking about with the FBI, it's ultimately the, you know, CISA is here to support the nuclear industry as well as all of the critical infrastructure industries in identifying or remediating vulnerabilities and identifying and remediating cybersecurity incidents and ultimately to help bolster the cybersecurity posture of the United States from a national security perspective.

And I don't think I need to explain to this audience why this community is critical to the overall national security. It doesn't need to be stated. But working with CISA is, you know, something that some of you have done. I can't actually see all the people that are on this call, but I'm assuming -- I know that some of you have worked with us and that have of you haven't, right? And so what's it like to work with CISA?

So we're a little bit of a different agency. Our kind of perspective and things is we're kind of support critical infrastructure and national security and so we have a lot of resources that can be made available, but may not, right?

The biggest misconception I think people have about CISA is that we will be there to save you and while we'd love to be there to save everybody, we can't save everyone, right? And really kind of our role is to surge towards the kind of most nationally critical incidents or issues that are occurring, right?

And so CISA is definitely here to help support in a backstop on a really, really bad day, but we aren't going to be your day-to-day

cybersecurity team. That's why you have your own cybersecurity team. That's why you should have your own resources. That's why you should work with your industry partners that can provide those services.

We are here to provide that kind of national level object. And that's something that I think is often kind of misconstrued about where CISA's role is in this entire exercise is that we're really there to just kind of mostly focus on is respect to nation state threats. And we're also working hand in hand with our partners at the FBI like Joel and I know each other well because the FBI is pursuing the -- kind of the adversary and they're there for the imposed cost portion which is a very important portion of how we deal with cybersecurity issues broadly. And then we're there to help with what we call asset response or healthy asset, kind of get better or get on a path to right in the near term.

So we are here to support and we do a lot of kind of broad messaging and stuff, and when you do have a kind of particularly bad day, we are here for you, but we shouldn't necessarily be your first call, but we are here to help. And we especially love when we get tip information from the private sector that

can enrich what we understand about what the adversary is doing out there in cyberspace. So I just kind of want to -- we're a little bit different as a federal agency. I just want to kind of set that record straight.

There is one thing that I want to talk about that Jacob mentioned during his piece which I thought was important and that's about visibility, right? So if you do not have -- and Jacob mentioned this and so I'm just going to double-tap it, it would be best to stop the bad guys from getting in your environment. But that would be what we would all want, right? But just the diversity, vulnerability, the diversity of risk, the complexity of some of these systems, that is not going to be successful one hundred percent of the time. There's just no way it's ever going to be a hundred percent capable and really detection is the next piece, right? And this is an area where we also see a lot of asset owner operators not have the detection capabilities that they need in their corporate networks and their control systems networks and can't tie the two things together, right?

Because from my experience and I've been doing it through response and control systems for like

12, 13 years now, most of the intrusions that we see come in through the corporate network, right? And so oftentimes you're going to have some reflections that you're going to be able to see in the initial intrusion phase that come through that vector. Before that, you get to the controls, right? Because at the controls systems level, we really don't -- we want to keep them out of there, right? I'd rather detect them when they're a little bit farther away from the level 4 access, right, I think would be the best thing in everyone's interest, right?

And so, making sure you have the detection engineering, detection technologies, and strategies in place is really, really critical and it's also really critical to ensure that you have behavioral, analytic techniques involved, right?

I would love to go through one meeting in my life where no one asks about indicators, because indicators -- well, they can be helpful, and they have a role and a place -- are usually the last thing I'm thinking about, right? I'm much more interested at looking at adversarial tactics, right? They move towards these types of assets in a controlled environment. They try and go after the

administrative user accounts, or certain actors like to target executive assistants because they tend to have a lot of access to mailboxes and files and systems in order to facilitate things, right?

And so like those types of tactics and those types of behaviors that the adversary have are things that we can fingerprint on, right? And I think we just got a really great example a couple of years, man, it feels like a couple of years ago, it was only like 12, 13 months now in the supply chain compromise that was SolarWinds. And I don't call it just SolarWinds because it wasn't just SolarWinds, number one. And number two, the adversary was using multiple intrusion techniques, not just supply chain compromise. So it was bigger than that.

But I think that was really instructive in behavioral analytic techniques, right? Because at the end of the day, the way to identify that you had a compromise in that particular case, yes, there were some indicators that the adversaries very, very quickly changed. They had one kind of call-back domain which was helpful, but in many of the responses that we did, the adversary quickly went to Bespoke per victim infrastructure for command and control.

And so IT addresses in domains and observables from there were useless to share with other orientation. It just wasn't going to happen, right?

And we've spent a lot of time kind of coalescing around information sharing which we often mean as indicator sharing and that is a very fragile way. And our adversaries have picked up that we've done that and they've moved to these types of more -- indicators are a lot more severable than they used to be.

And so by looking at and having your detection engineering in more of a tactic space kind of concept, you're going to be much more successful at catching the things you don't already know to look for. I'm not saying don't look at -- for indicators. You should totally look for indicators because you want to catch that low-hanging fruit, but especially for an industry that if somebody wants to hold at risk is definitely a little bit more weighty than holding at risk a small water utility somewhere. Right?

Someone hacking into nuclear reactors or nuclear fuel cycle facilities, you know, that's a horse of a different color from an adversary perspective, and you know, you're likely -- you're

more likely to come against the A game than, you know, the Oldsmar water utility, as an example, right?

And so focusing on behaviors and tactics is going to be a much more useful thing to catch that zero day type exploitation activity, right, and looking at user behavior patterns. Why is Bob logging in from two places at once? Hey, let's have help desk call Bob and find out if he's really in two places at the same time.

It might be true. It happens to me all the time, so -- but anyway. It's really about behaviors.

And I will mention one thing that I know some of you worked with us on, one of the things that CISA is trying to do is kind of give that national perspective on behaviors, right? And we're trying to better understand what our adversaries' capabilities, plans, and intents are and how well positioned they are to hold U.S. assets nationally at risk.

And so one of the ways that we are doing that is getting some additional visibility and we're doing that kind of in two different ways. The first way that we have and it's something that we call CyberSentry. It's a new platform that we have that -

- turning into a full program, we've been piloting it for a little while with some nuclear reactor operators. I won't name who they are. You can ask your friends and see if admit to it, but basically what we've done is put a rather extensive sensing sweep that the government provided into the control system environment and into the corporate network environment on the inside of the firewall to be able to get that telemetry from both those places and look at that.

And we're using CyberSentry to cross correlate across multiple sectors in very, very, very deep data webs, right? And it's not a program that's for everybody, but it is something that we are kind of now talking about more and expanding to provide an over-watch capability into your environment. Again, it's not something that's for every applicant or operator, but kind of going back to my first point, it is absolutely in addition to what you are already doing for your security. It's not supposed to replace your security. It's an over watch, right? But it allows us in CISA to use some more bespoke analytic procedures, such as things that we can't necessarily do at scale in a sharing way and we can then look for

those types of things, right? And it's been rather successful in catching some interesting adversary activity that I think go in to a very different context.

The second thing that we're doing from a visibility perspective is partnering. So we've lately in CISA been working with a variety of managed service providers or vendors. Jacob is from Dragos and we announced recently that they were the first one that we've actually gotten through the hoop on this, but we are working to work with those managed service providers to get access to -- query some of their telemetry and some of the data that they have, right, because CISA like CyberSentry is kind of the thing we have and that gives us lots of deep insight, but we can't put it everywhere, right? And so one of the way that we're trying to scale is working with managed service providers like Dragos on the OT side, but then also others that I can't mention because we're not actually done the process yet. But it's not just them. We're working with several other vendors of a similar line to work with them on some of the telemetry exchange so that we at CISA can kind of get a better sense for what's actually happening

across multiple critical infrastructures domestically.

So that visibility piece is super important for you and it's super important for us just kind of different visibility.

The last thing that I want to touch on before I'll hand the mic back and we'll get into Q and A and I just got to address it, right? I mean so many of you live in interesting times, right? You know, what's going on over in Ukraine -- and someone who has been there on a number of occasions, it's heart breaking and you know, as a person, it's a little tough to watch in some instances, but it is important for this community to understand that just because it's a third or so the way around the world doesn't mean it can't come home, right?

One thing that CISA has been really trying to espouse and I know our colleagues at the FBI have been doing this as well, is you know, it is in times of heightened tension where adversaries start to look for other tools to influence geopolitical situations, right? And so, if you have an adversary, and you want to keep America out of a war, they're going to start to look for tools to do that and some of those tools

could be things like going after critical infrastructure in the homeland. That's a rational thought by some threat actors, right?

And so this is a great time to think about your security posture as it relates to potential nation state intrusions and whether or not you're comfortable with the level of risk you are managing in your environment.

Now it is not a time to panic. I can't stress that enough. You know, the war that's happening over in Eastern Europe does not suddenly make more hours in the day and does not make -- you know, if you weren't doing good logging yesterday, starting a logging program is a great idea now, but you're not going to implement it in 24 hours. Don't burn out. But it's a good way to reflect that hey, if someone wanted to use bespoke capabilities against my environment, would I even notice? How would I notice? Have I tested these hypotheses? Have I actually done a hunt? Are they already here, right?

These are the types of things that these types of geopolitical tensions are great reminders that we do live in a broader world and sometimes that broader world wishes to do us harm and it's kind of

our job to blunt that harm. And if we can't stop it, at least minimize its impacts and detect it early, right?

And so, that's just the thought I'll leave you with is just to take 30 seconds to think about your risk posture and if the best possible adversary that you can conceive of was coming at you, would you know, right? That's a really great question to ask.

Anyway, with that, I'll let you ask questions. So I'll kick it back over to you, Jim, because I think you're the moderator.

MR. BEARDSLEY: Thanks, Mark. So at this point we have a number of questions we're going to ask the panel and some of them are specific, some of them are for the whole panel.

So the first one is for the whole panel and I'll ask Bob to kick it off, but the question is what do you see as near term or over the horizon threats to industrial control systems or the nuclear sector and how might they differ from what we've seen in the past?

Go ahead, Bob.

MR. ANDERSON: So I would say initially supply chain is obviously one of the top ones that we

have been focusing on. There are so many aspects to supply chains. It's really difficult to nail it down here from the cybersecurity perspective. But what I really want to shift to and I really feel this pretty strongly is with the Silver Tsunami that's happening in the nuclear industry, I really think the people are one of the biggest areas that we need to focus on and again, not to beat my own drum here, but cyber-informed engineering and other cyber-by-design processes and different education that's available to engineering types and others on cybersecurity is going to be imperative in the future coming up. And so I would give those two equal weight.

MR. BEARDSLEY: Okay, any other thoughts?

MR. MAX: I think one thing the FBI has seen in the short term currently is just the increasing use of ransomware. This isn't new to anybody, but I think what is concerning to us when we look at some of these threat groups is that there are specific ransom variants that are not specifically targeted solely at ICS systems, but have aspects that can affect control networks, and so as these actors become more aggressive and go after different targets, that's one area I would be concerned about, not

necessarily even because of an intentional attack on your OT network, but something that spills over. We've seen that quite a bit in the water sector. A number of incidents that started on the IT side and just spilled over into OT due to poor segmentation, that resulted in facilities having to go to manual operations. So I think looking at that as a threat is really important, especially when a lot of these groups are -- they're not really state -- they're not affiliated with a particular nation state, and so they're able to operate in a space that's much harder for the U.S. Government to impose risk in and consequences of these actors.

MR. BEARDSLEY: Thanks, Joel. Other thoughts?

MR. BRISTOW: Yes, so I wanted to second the Gray Tsunami comment. I think a number of sectors are having that same crisis of expertise. And that is something that is -- you know, if I was listing the risks to most critical infrastructure sectors, that would probably be at the top or near the top of every single sector plus.

As a younger, but feeling old kind of guy, I guess I can -- I'm looking forward to being part of

that problem, but yes, it's definitely a big thing. It's been my observation, you've got a lot of operations and years in there and kind of 50s and 60s and then like a huge gap, and there tends to be like some maybe 20s and 30s kind of range. Then you get a sector maybe a little bit of an outlier there, but there's not a lot in the middle which is, I think, part of the challenge.

You know, I think though the thing that I see as -- and it's not a risk right now, but it's one that -- and I know that the NRC is working on this, but it is -- the nuclear sector used to be one of the sectors that I quite frankly stress less about than some of the other ones. And part of the reason was is that quite frankly why I definitely care deeply that, you know, business networks and that kind of stuff get compromised, at the end of the day the way most nuclear power facilities operate are, you know, electro-mechanical controls and things that ultimately don't have a lot of cyber risk. And so from a part of the infrastructure that like from my chair at CISA I got to make sure it still works. You know, I didn't have as much risk as I did in other sectors with more pervasive control. But as digital

controls are becoming more of an item in the nuclear sector, that is something that is going to change that equation and stuff that I don't have confidence that it won't be done well, that's not that what I'm trying to say at all, but during any time of transformational time, we're bringing in new risk sectors is something that has to be done very softly and very carefully and this will be effectively bringing in some new risk factors that were not really widely available to nuclear. It used to be people would ask me, like oh, yes, it would have be nuclear power, but like, no. That's like not okay, right? You know, it's like with a wrench? Sure.

But now, we're -- there's some things. And so I think that while many as the owner operators have robust cybersecurity programs, there's just going to be more risks on the table than there was before as transitions happen and that's going to be something that the industry as a whole is really going to have to work with.

MR. BEARDSLEY: Thanks, Mark. If there are no other thoughts on the first question, we can go to the second one.

DR. BENJAMIN: I have a thought on the

first question.

MR. BEARDSLEY: Go ahead.

DR. BENJAMIN: And just to -- it's a bit of an echo of the two comments is that it really truly, it's two different problems that when together makes the problem worse, right? So you've got the Silver Tsunami and then you've got the rapid digitalization. And so when those two things are happening at the same time, something goes wrong. The expertise isn't there any more to answer, to go back to the manual controls and things like that. That would be a worry there.

And then in general, too, a little bit on the horizon is just attacking nuclear for the sake of not necessarily thinking you're actually going to get in, or get through, but you're attacking the reputation. This combines with the Silver Tsunami like the people will lose faith. Do we really have this under control? And then we have to start thinking about where we're going to get the other percentages of our power, our power generation, right?

And that's one part of it and then combined with its -- slightly recently, it's just this -- it's sort of recent disregard for safety, right?

At one point you would think it would be out of the realm of possibility that somebody would specifically target a safety system to hurt people. And we saw this with TRISIS in 2017 over in the Middle East. I know that wasn't nuclear, but it was an oil and gas facility, right? We saw this lack of disregard for safety.

And similar recent events is well, we're seeing similar situations, right? And so that combined with everything is certainly a threat I'm thinking about on the horizon. So thanks, Jim.

MR. BEARDSLEY: Thanks, Jacob. So our next question is for Jacob to start and then we'll see if anyone else has any thoughts.

Jacob, you indicated from 2021 key findings on the front line, 77 percent poor segmentation.

Can you speak on the lessons learned or suggested improvements for segmentation?

DR. BENJAMIN: Absolutely. So segmentation as a whole, this specific metric here is mostly talking about facilities that don't have hard breaks, like nuclear has. And so for those organizations, I would talk about implementing

something similar to a hard --- I'm not saying everybody needs a hard break, but validating this segmentation.

I'm a big fan of doing it through software-defined networks. I think they're easy to maintain and I think they're wonderful. I'm a big fan of software-defined networks.

I think Bob will probably like this answer and this is specific for nuclear, I love the IAEA approach of zones and levels, zones within the levels. So one thing you see often in the nuclear, right, we have the four network levels. And then oftentimes, you get into one of the network levels and you can communicate to anything within that network. There's not any horizontal controls, if you will, or many places lack access controls if you will or many places lack access control lists and things like that within the level. And so you have to kind of assume that whole level is compromised if that level gets compromised, right?

And so would love to see more horizontal protections in addition to those vertical breaks that we are seeing between the network levels. So I hope that helps.

MR. BRISTOW: I second that.

MR. BEARDSLEY: Any other thoughts?

MR. BRISTOW: No, I -- no. That's a really important point and thanks for bringing that up is that like there's nothing that exploitation engineers like more than once they get in, they can move anywhere they want inside that environment, right?

And so lateral movement is definitely something that you need to be able to not only detect, but then if you can create segmentation, you know, I hate to use this term, but Zero Trust, you know type of -- I always call it real time, authentication authorization, but it doesn't sound as good. But no, those types of principles though are really, really valuable in locking on a network and constraining an adversary. So if they get in, they only can go so well. It's a really great point.

MR. ANDERSON: I would add also back to Jacob's comment about levels and zones, that we need to keep in mind that when we look at security levels, it's all about the functions that we're trying to protect and those control systems that provide those functions and so I see it as a graded approach where

we really want to make sure that those critical functions are protected at the highest level and then we work down from there on those functions that may be less important because, you know, we all have limited resources and we can't protect everything at the highest level.

And so, yes, I really agree that levels and zones are really important as part of that segmentation.

MR. BEARDSLEY: Thanks. So our next question was specifically targeted to Joel, so we'll start with Joel and we'll see where it goes from there.

Joel, we often read about cyber-attacks, but rarely do we hear about hackers being caught or convicted and punished. Are hackers getting arrested?

MR. MAX: So the short answer is yes and no. When it comes to a lot of our -- like the cyber criminal side of the house, we've had much better success getting handcuffs on bad guys. The truth of it is that when we're talking about our nation state adversaries like China and Russia, it's much more difficult to actually ever arrest somebody and bring

them to justice that way.

However, one of our new, kind of our pillars within FBI Cyber Division is about posing risks and consequences. And so in the cases where we cannot maybe effect an arrest when we would like to, we try to impose that -- costs in other ways. So for example, we recently, well recently as in last year, released indictments against a number of GRU officers for a state of different attacks to include Ukraine 2015-2016. And these type of indictments are useful in that these individuals are sanctioned. They can't travel. If they're here, could be potentially extradited, if they leave Russia or a similar country. It also eliminates the prospect of getting work in the West and other places. We've seen this with China recently with some of the indictments related to some of the COVID research, with some of the vaccine research, so the FBI and its partners at the Treasury Department and our international partners have really been working to try and impose costs that way.

There was a note, we on a few occasions got lucky and have been able to work on gaining some extraditions, but it really is difficult nowadays when you're talking about a state actor.

MR. BEARDSLEY: Thanks. Okay, our fourth question and this is for everyone, so if you hear it and you want to jump in, let me know.

Do you see any best practices in other sectors as the nuclear sector might want to leverage in its cyber defense?

MR. MAX: I guess I'll go first. Just to kind of bring up a point I mentioned earlier and I think that everyone on the panel has mentioned so far that you know, really, we're in the age of really needing to have a good asset inventory, to have a good baseline with your system because trying to understand that native, all different native functionalities you may use in your networks and how the adversaries can use those back against you, I think that we've seen in some of our engagements with industry some folks are doing some really innovative work in doing baseline and understanding network activity, user activity, things of that nature. So I think that really is one of the keys that we've seen.

MR. BEARDSLEY: Other thoughts?

DR. BENJAMIN: I had one as well. So -- and it's difficult because for a long time I've always considered nuclear to be a part of the electric

sector, but I guess sometimes we're separate and sometimes we're not, right?

And so the electric sector is doing such a great job with information sharing. The E-ISAC and things like you alluded to earlier with our neighborhood keeper where they can send anonymized information sharing of analytics to government agencies or to others within the program as well. It's just -- it makes it more of a team, right? It's not just the small co-op that's battling a nation state. It's all of us together, right? And that helps us scale and things like that.

So I would say the information sharing in a technical sense, because nuclear has always done a great job of sharing information with each other like in a non-technical way, right? Like the foreign states have been wonderful. But specifically, like with the analytic sharing that we're talking about with like neighborhood keeper.

I would say that and actually within data centers, too, we've been doing a lot of building automation assessments and they have really robust and centralized logging that's very easy to then go through and do hunts on. So a big fan of that and I

would like to see that more so in the nuclear sector.

MR. BEARDSLEY: Okay.

MR. BRISTOW: My point would be because I think actually nuclear is doing a lot of things right, but one thing that -- especially segmentation, like from a big block segmentation that, that's been -- that kind of standard that I point to for other sectors. But one place where I think more focus to be is an identity, so identity, identity is the new perimeter and I think that especially as we move to more as a service provided capabilities and those sorts of things like identity starts to become more important than assets. And I have not seen as much focus in the nuclear sector on identity analytics and identity management it has in other sectors. And so that's one area where I think nuclear could stand to improve a little bit.

MR. ANDERSON: I would just add, too, on the information sharing part that maybe a little more threat type information sharing would be helpful, too, because that's very, very closed within the nuclear industry and again, I remember several years ago at the IAEA we were talking about how to increase some of that threat-sharing information, whether there's a

neutral broker, you know, for everybody or not. And it just was very difficult. There's too many issues that surround that and so yes, I just think there should be some way to be able to share threat information better.

MR. BEARDSLEY: Okay.

MR. ANDERSON: I do know that there's a lot of big government efforts to try and look at sharing information, working with industry, working with IT companies. That doesn't necessarily help in the OT environment, but we have to start somewhere and as that starts to mature, sharing that with the nuclear industry is something that would be very important. It's something the NRC is keeping is on as well.

MR. BEARDSLEY: Okay, next question. This one is targeted at Bob, but we can have anyone speak to it after that. It has been asserted that the use of Field Programmable Gate Arrays will lead to increased security postures at nuclear power plants. Can you provide some brief thoughts on that?

MR. ANDERSON: Yes, so for sure it increases security, but it's not the silver bullet one hundred percent. There, we still have to deal

with different times of FPGAs. Some of them actually incorporate CPU processing on them, so it really depends what type of FPGA that you're using. Our lab has found some vulnerabilities within FPGAs. It may be a little more difficult to exploit those, but a few of them do exist. And then you've also got data streams that you have to worry about that gets propagated into the FPGAs. So there are some areas that need to be looked at, but it definitely does supply -- provide an extra level of protection, I guess.

MR. BEARDSLEY: Okay. Other thoughts?

MR. BRISTOW: Yeah, I think that, again, FPGA technology is one that can bring a lot of value. But it creates new expectation pathways as well, right? And again, it's all about the context in which things are deployed, right, because where before a set of circuits is only going to do a thing, right?

Like, physics kind of says it's only going to do a thing. And you degrade or destroy it. But you can't really make it -- you can't make a circuit design to tell time, to cook your breakfast. It's just not going to work, right?

Even FPGA is designed to tell time to make

you breakfast. I know. I made an FPGA in school that ran a robot that cooked food. So it was a project in class, right?

And so because they're programmable and they're reprogrammable, it starts to become a conversation about the management backplane on how, like, how programmable are they. Just like RPLCs and RTUs, right? Like, if an adversary can get into the -- the logical extension is we'll want to -- they're great so we can reprogram them. So we're going to use them.

We're going to make it available to reprogram them on the fly to increase efficiency which means they get put on a network which means they then can get rid of a reprogram by anybody who has the appropriate credentials on that type of environment which I go back to my comment about identity being the new perimeter. So I actually -- I love FPGAs. Don't get me wrong.

I think I'm a big fan of the KISS concept of, like, falling back to analog. Actually in a lot of instances might be something really useful to do in a lot of contexts. But again, we just got to think about making sure that we don't fall into some of the

same traps we've falling into previously.

MR. BEARDSLEY: All right. So our next question, this is for everyone. So what can non-IT/OT staff take -- what role can non-IT and OT staff take in detecting and responding to cyber incidents.

DR. BENJAMIN: So I can start off if you don't mind. We see a lot of this with our -- we do a number of incident response tabletop exercises all across the industry, right? And so we see cross-organization help.

So sometimes it's just bridging the gap between IT and OT and making sure everybody is in the same room. Sometimes it's like whether it's creating a RACI matrix and making sure everybody's roles and responsibilities are thought out and known. We have a defined incident commander, and we're following the documentation of our incident response plan.

And some of it might be just making sure you have an incident response plan. I know all of you do because it's required in the Reg Guide. But for some industries, they don't always have that.

And so just testing that incident response plan and going through, you don't necessarily have to be an IT person or an OT person to do that.

Ideally, you're involving others. You're involving the entire organization. And I think Bob has got to follow up on this as well. So I'll pass it to Bob.

MR. ANDERSON: Yeah, I would just say who uses cell phones out there? Like, everybody. I'm seeing all the hands going up right now, right? Do you use a computer? Of course we use computers, right.

So I think education is huge, and it's for everyone. It's not just for the IT/OT folks or technical people. But it's even your administrators who do a lot of that pre-processing for a lot of us within our email system and all. So I really would push high that education on cybersecurity is huge for every organization.

MR. BEARDSLEY: Okay.

(Simultaneous speaking.)

MR. MAX: I'd like to add too that I think having really fulsome discussions with your executive management is critical too, whether that's your C-suite or your board or folks that have -- are in the position to, one, give you resources, but two, also are the decision makers when you're going to be in an incident. We recently worked with a private industry

partner on a tabletop where they had their board of directors work through a ransom incident of who are we going to call. What are the procedures?

What does that look like exactly? And I think having -- kind of giving that a little bit of education about what that looks like from all the way down the line level up to that executive level. It's absolutely paramount.

MR. BEARDSLEY: Okay. So the next question is sort of circling back to something that was mentioned. It's been mentioned a couple of times. But it talks to supply chain. And strategies for dealing with the increasing roles of supply and cyber defense, giving off the sense that it's beyond the operator's control, what recommendations would you have to an operator in trying to shore up their supply chain cyber defense?

(Simultaneous speaking.)

DR. BENJAMIN: Go ahead, Bob.

MR. ANDERSON: Oh, maybe I can start first because I work a lot with the IAEA. They just put out a technical document called computer security approaches to reduce cyber risk the in the nuclear supply chain. And so I would highly recommend that

people go and find that and download that and see if that might be a really cool tool for them.

DR. BENJAMIN: I would echo. Definitely check that out. One thing I wanted to say is one thing that we see a lot as we are responding to SolarWinds last year on a number of these active cases that we're responding to is oftentimes the asset owner couldn't answer.

We were unable to answer the hypothesis of whether it was compromised because they didn't have the data. They didn't have the logs. They didn't have the -- you needed three months' worth of data to identify whether it had been exploited. And they only had seven days' worth of rolling logs, right.

And so understanding that you need that information, especially the timeline for supply chain attacks being much broader, right, or being longer, sometimes 9 months, 12 months out. And so you need longer windows of logs to be able to then go hunt and see those things through. So one thing we're always mentioning is building out a collection management framework.

And that's basically a table, a dossier of devices on your network, the data that they have,

how important that data is that for what questions you might try to answer and then follow up, right? Like, so I checked this firewall to get this answer. And then my follow up is the registry of this device over here. And so just having all of that ahead of time really can speed up the incident response situation to hopefully you can shrink that window and be able to answer your hypothesis. Thanks.

MR. BEARDSLEY: Other thoughts on supply chain? All right. Next question. We'll load it up. Okay. So this is, I think, for everybody. All right. So I'm going to take a first crack at this one and then I'll ask Mark to jump in.

The question is, is it possible for the NRC to get private industry notifications for incidents that may involve nuclear reactors? And if so, how will we go about getting on that list? Well, first of all, the nuclear power industry has a regulatory requirement to report any cyber-attack to their safety security emergency preparedness systems to the NRC.

And even possible cyber-attacks they have a requirement. If the NRC received one of the requirements, we would turn that around as quickly as

we could and inform industry. So that's a service that we will provide.

We also rely on the second risk management agency for the nuclear sector which is part of DHS CISA to share the alerts that come out of the cybersecurity part of CISA. And if there's any entity in the nuclear industry that is not part of that communication stream from the sector risk management agency, trying to recommend that you get on that list. And if you don't know how to do that, please reach out to us and we'll help you. Mark, any thoughts?

MR. BRISTOW: Yeah, so on the second part, absolutely. We put out a variety of alerts, not always public that are oftentimes we have some security controls that are in place around it. So we'll have, like, different -- we use the TLP, traffic light protocol, standard for articulating. So it might TLP green or TLP amber. If you don't know what that is, you just go to US-cert.gov/tlp, there's an explanation.

So when it's more sensitive, we will put it out kind of on our mailing lists. You can reach out to CISA at central@cisa.gov to get signed up for those alerts and get on the right mailing list and

those sorts of things. Or you can reach out to your NRC point of contact. Or if you have a CISA point of contact because we do run the SRNA for nuclear, they can also do that for you as well.

But yeah, there's definitely lists to get on. But I will say broadly speaking, we strive to put as much out as we can just TLP White or public because we realize that our lists aren't going to hit all the right people that need to get the information ever. And so we strive to kind of hit the public surface as much as humanly possible.

But in some instances, it's just not -- their sensitivity is just not possible. But anyone in this industry can be signed up for, like, the TLP amber stuff. That's not a problem.

MR. BEARDSLEY: Okay. Any other thoughts. I know this is sort of specific. But anyone else? Okay. So the next question came in from the system, and we rephrased it a little bit. And we may have already talked to some extent. But what are your thoughts on protecting from zero-day attacks?

DR. BENJAMIN: I mean, it depends on the attack, right? But in general, this goes back to

something Mark was talking about before in that not putting all your eggs in the IOC basket, right? So focusing on more resilient threat detections, focusing on things that are hard for the adversary to change.

So you look at -- I think David Bianco created this pyramid of pain, right? So you've got indicators. You've got domains that they need to change. So whether you're changing the hashes or the files, the domains they're using, the infrastructure.

And eventually, you get to a point it's very difficult. They're always going to want to do initial access, grab credentials, and pivot off that device to another device and call home from that device. That's not changing.

That might change once every two years as opposed to a month or a week. Some of these indicators are really only good for a very short amount of time. So I would say focus in on those resilient behaviors are going to help you with the zero-day attack as well as making sure that you don't have this prevention mentality that -- and actually, for a long time, I felt nuclear did.

You hide behind the data diode. You

don't want to do anything else. And the data diode is not a silver bullet, right? And so at some point in time, you have to make sure that you have other controls.

It's not just prevention. You're also doing the recovery and response and detection pieces of sort of like the NIST framework, right? There's more than just protect.

And so just making sure that you can facilitate all of those, not put everything in the prevention basket. Understand that prevention is ideal but not guaranteed. And you will need to be able to detect and respond. I'll pass it to Bob. I think he's got his hand up.

MR. ANDERSON: Yeah, I would also come back to the people answer that if you don't have people looking at the logs and looking at your alerts and things that you have and looking at the data traffic, things can go by that you may not see, depending on how good the zero-day is. And so again it comes back to the people doing the jobs that they need to do. And there's a lot of tools out there obviously to help sift through all that traffic. But if you have people who are trained and educated that

are looking for some of those suspicious patterns, I think that's just as important as all the technical stuff.

DR. BENJAMIN: And you need visibility to know what normal looks like. So when abnormal happens, it's not is this a process anomaly or is it a cyber event. You know, hey, this is weird. My PI Historian is sending commands directly to a PLC. That's strange and that probably shouldn't happen, right? And so knowing that and then keying in on that is definitely key.

MR. ANDERSON: Yeah, absolutely.

MR. BRISTOW: I know. I think those are really important points. That's weird is probably the scariest thing you can hear from one of your analysts. Okay? Why is it doing that, right? That is -- everyone always thinks that when cyber-attacks happen, clock times go off and those types of things, right?

And it's really some analyst going, that doesn't make sense. I don't understand that. At least it's broken some of the most consequential cases that I've worked.

But again, I just want to just drive this

point home too that you can only see weird if you know what normal looks like. And you can only see what normal looks like if you have good visibility, right? And Jim mentioned you have a collection management framework, understanding where your visibility is, where it's not.

Those are the things you need to preposition. And that's stuff that you can do now, right? Can you defend yourself from a zero-day? You can maybe, maybe not.

But what you can control is whether or not you can position yourself for success. That you have control over, right? And so making sure that you have logging, that you have a SIM, that you have well trained analysts. Like, these are all the prerequisites to repelling unique or big scope attacks.

MR. MAX: And I want to just do a quick call to CISA. It's a really great resource that says it publishes every year. It looks at the top ten vulnerabilities that we see exploited.

And maybe times, these -- you would think that advanced actors are using some sort of exploitive tool when oftentimes they're using the most readily

available exploit. So I would encourage everyone go to check that out. There's also a number of resources that are tied to each of those exploits in terms of mitigation.

MR. BRISTOW: Yeah, thanks, Joel, for the shout out. And I'll just throw out a little bit of extra balm on that one. So we recently started putting out this thing called the KEV or the known exploited vulnerabilities list which is in the federal space, they're required to fix these vulnerabilities first.

We recently put out I think 91 vulnerabilities on the KEV, like, tail end of last week. And some of them were from 2000 and I think they went back to 2004 because they were being actively exploited, like, now. So I can't stress that point that Joel brought up which, perfect point, enough that, like, you think nation-state and, like, high order actors are using only the new hotness.

So you don't get extra points for the cool hack. They still have bosses and spreadsheets and budgets, too. So, like, if a 2004 vulnerability will make it work, that's what they're going to use and that's what we're still seeing in some environments.

DR. BENJAMIN: I would just echo one of the number one credential dumping tools that we still and our activity groups still use -- I brought it up earlier today -- is Mimikatz. Mimikatz was released in 2007. Still works. Still super valuable. That's not changing, right?

MR. BEARDSLEY: Okay. Good discussion. Next question, this is for everyone. What are your thoughts on risk informing the selection of digital assets that need to be protected or subsequently the level of protection for the assets?

MR. ANDERSON: So maybe I'll start on that. We have our design basis documents. We have our tech specs. We have our safety systems -- safety-related systems.

Of course, those would all be things that you would want to look at first. And then you work yourself down to just what are those systems that may even influence some of those safety systems and work yourself backwards. But I think there's a lot of documentation that already exists out there and trying to identify what those most critical functions are. Jacob?

DR. BENJAMIN: Yeah, I would just -- what

you said, right? You can't protect everything the same. It seems unreasonable that I would protect a chart recorder the same level I would protect a safety system. That doesn't make sense, right.

And so definitely making sure that we're applying controls as appropriate, right? We have limited resources. I'm glad you said there's a number of publications out there of how to go about identifying that and doing that. But definitely a graded approach and a risk informed approach is the way to go.

MR. BRISTOW: Yeah, no, I completely agree. And you cannot protect all the things. It's just, like, not a doable thing. And so you have to prioritize. You got to prioritize.

But remember to prioritize like an attack, right? So yes, one mistake I often see people make when trying to make risk informed prioritization decisions is they're thinking about what's important to process which is important.

But you got to also think about what the attacker's kill chain looks like and what type of techniques. Again, I'm going to back to TTPs, the tactics, techniques, and procedures. What TTPs the

adversaries are using to get to those assets, right?

So your chart recorder might not be, in and of itself, particularly important. But if it's a pivot point into the environment where compromising that can give you access. It's maybe a little more important than it looks, right?

And this is where I love using the MITRE ATT&CK and MITRE ICS ATT&CK lexicon for overlaying onto your collection management framework or where you can see what tactics are being used by adversaries broadly. And then can we see those tactics, right? And then that will start to show you what assets in your environment actually are critical to the attacker's kill chain, right?

Because it's not just what's important to the process. It's also what's important the attacker's kill chain. And that is not -- that's a Venn diagram, not a circle. So you got to take both things into account.

MR. BEARDSLEY: Okay. All right. So the next question is a little more open ended. As new licensees, small module reactors, and advanced reactors, licensees look at incorporating technology such as wireless networks for autonomous control, what

recommendations would you have?

MR. BRISTOW: So I'm assuming that there's a lot of engineers on this call, right? I'm just going to put that out there, right? Like, nuclear engineers, but, like, everyone takes, like, basic EE courses, right, at some point, a computer engineer education. But like D squared, right?

So, like, energy dissipates over D squared. It dissipates, but it doesn't go away, right? Like, wireless can be hacked from space just so we're all super clear.

So anything you put over a wireless, just understand that there is no way that that signal is private, can't be denied, and can't be intercepted. Or integrity can be maintained on the wireless signal. Now you put things on top of it that can maybe increase that security level.

But, like, wireless goes on forever, right? Over D squared, never actually hit zero. And so that's something to really think about. And in more true DCS type environments where you don't' have a large physical footprint, fiber doesn't cost all that much. And it's -- you can't hack light from space, not inside a little glass tube.

DR. BENJAMIN: Just to follow up, I did a number of research on ICS while I was at Idaho National Lab. And when it comes to, like, autonomous control, that's a big yikes for me, right? I'm not a big -- I'm with Mark on the space hacking there.

And however when it comes to plant optimization, so polling data to help with preventative maintenance and things like that on non-safety systems, on systems that are maybe important for efficiencies but not important for safety and things like that, I think that's fine. I do say just roughly -- I mean, I haven't looked at it in a couple years now. But when we were looking at it before, there was one plant implementing wireless, and the plant was something like 50 million dollars.

But then implementing, like, a DAS LTE override was maybe one or two million dollars. So there is significant cost savings from going there, right? So there is reasons to look at it. But I would hesitate to do anything on the safety side or control side. But I would be okay with some kind of controlled plant efficiency operationalization that way.

MR. ANDERSON: So I would just add that

as far as an autonomous operation, baby steps would be a good thing. What we automate or do that automated control on might be another thing we want to look at. And that kind of goes with wireless too.

Maybe there are some places that wireless makes sense. But there's certainly other critical functions that maybe it's not such a good idea. So that's it.

MR. BEARDSLEY: Okay. Other thoughts?

(No response.)

MR. BEARDSLEY: All right. I have one more question. Let's see here. And it sort of plays off some of the discussion we had earlier, but I'll go for it. Can you talk about the importance of hardening devices in order to facilitate understanding and identifying normal traffic and behavior?

MR. BRISTOW: Yeah, so understanding normal is probably one of the most important things you can do. It is the least sexy thing you can do in cybersecurity but it is the most important thing, right? It is part of the set of brush your teeth and eat your vegetables which I could use a little bit more vegetables.

But it is -- if you don't know what's supposed to be happening in your environment, you're not going to be successful. And another thing, some analysis that NSA, FBI, and DHS, it was insisted and put out a couple years ago that every time we go back and check it's still true. We put out the seven steps to effectively to defend industrial control systems.

And when we do that initial analysis, one of the things that was a little shocking to me was when we looked at root cause analysis of incidents that happened broadly across control systems environments, allow listing applications or formerly known application whitelisting was actually the number one control that would've stopped the most things. And while it is by no means a silver bullet, just like multi-vector authentication, super useful tool, not a silver bullet. That is a hardening thing that requires you to understand your baseline and what applications in software need to run on your system.

And then make your system only run those things. And then when you come in to bring in malware or other code, don't get me wrong, especially identity, this doesn't help with that. But, like, stops a vast number of different intrusion

capabilities.

And if you've ever gotten an email from me, at the bottom of my email, it says, how'd you frustrate the adversary today? It's my tag line. It will definitely frustrate your adversary if they can't execute anything new on your system. So hardening and baselining kind of go hand in hand and are just of paramount importance.

DR. BENJAMIN: So on the flip side to that from some of the lessons I've seen in the field, I've seen situations where the way it's configured the vendor actually doesn't allow -- they almost do the opposite where the data software and everything there, that folder and everything is actually whitelisted from the AV that's installed on there. And so it makes a great staging point from my fantastic malware that we use for things, right? And even then when we're looking at group policy, hardening and things like that, oftentimes, you'll see some privileges that are there that don't need to be there.

One of my recent favorites was the SeImpersonate. You can use this juicy potato exploit. It's one of my favorites to immediately get system level access -- not just administrative by

system level. And so I've seen it. Just, like, we would look through different networks. And several of the computers on that network didn't have that.

But we found one that did. And then we were able to exploit and then obviously stage malware in the whitelist directory there. So I would caution that it seems like we do have to get vendors on board with this approach because a lot of times, the asset owner's hands are tied and they're not allowed to configure and harden them to the way that we would like them to be. And so getting the vendors on board to help us with that is a big step.

MR. ANDERSON: I would just like to add a reminder that operational technology is pretty easy to know what our traffic looks like. It doesn't change very often. I mean, we have these systems running for 20-plus years.

And so yeah, absolutely we can totally whitelist or whatever we need to do because we understand what the traffic is. It's a lot harder on the IT side. And the other comment I would make on hardening is, for me, that's just a hygiene issue. Everybody should be hardening their systems no matter whether it's OT or IT side.

MR. BEARDSLEY: Thanks. Any final thoughts? Okay. I'd like to thank this session of participants and all those who logged in to hear the discussion. We hope you found this subject matter interesting and had a greater appreciation for the potential challenges of cybersecurity for industrial control systems.

I'd also like to thank the NRC's RIC team and the contractors that made this session possible. It went very smoothly and we really appreciate it. Finally, I'd like to thank my support team for the cybersecurity branch: Tammie Rivera, Brian Yip, and all the other branch members who helped participate, came up with the idea for the session, helped us put the session together.

And Tammie and Brian in particular did a lot of leg work, making a lot of phone calls, sent me 100 emails making sure I was paying attention to what I needed to do.

Thanks, everyone. With that, I'll close out our 2022 Cyber RIC session and wish you all a fine evening.

(Whereupon, the above-entitled matter went off the record at 4:29 p.m.)