Transcript

Integrating Emerging and Cross-Cutting Technologies: Cybersecuity Across the Disciplines with John Sands

SPEAKERS
John Sands, Mike Lesiecki

Mike Lesiecki
Our series on the Future of Work is continuing with the focus on integrating emerging and cross cutting technologies. We are hearing from educators on exactly how they are creating changes and new opportunities for learners in partnership with industry note that this presentation does not necessarily reflect the views of our sponsor, the National Science Foundation. A video version of this presentation is available on our website Preparing Technicians dot org, it is now my pleasure to welcome John Sands from Moraine Valley Community College. And tell us a bit about yourself done personalized yourself you got a lot of experience in this field. You've been doing this for a long time. Yeah,

John Sands
Mike Lesiecki, I've taught at Moraine now going on 36 years. And I've run the CSSIA center with a colleague of mine, Eric Spengler back, we started in 2002. So we've been working with NSF from the 1990s. And we've been working in cybersecurity, and community colleges since 2002, 2003. So what I'd like to do today is talk about cybersecurity, in this area of the Future of Work. So, one of the things that we are very focused on as part of the NYcTE center is helping institutions across the country incorporate cybersecurity across the curriculum. And what I'd like to do this morning is talk about why is that necessary? And what are some of the approaches and some of the barriers and things that we as a center can help schools with, and it's a two way conversation, so we talk about how we can help them. And I have to be honest, they talk about how they can help us and better preparing our cybersecurity professionals to work in different environments and different disciplines. So it really is a great opportunity for both cybersecurity educators and educators from other disciplines to get together and really think about ways that we can improve cybersecurity education and how we can actually design content that can be used across

Mike Lesiecki
the curriculum. John, I heard a lot of good things about that conference (CYAD) last year it was in Chicago, will it be in Chicago, again at Moraine?

John Sands
Yes. So we will be hosting it again this year, in mid June. It's a two day conference, it's held at Moraine Valley Community College, and we, you know, we keep the cost very low for that. I mean, the cost basically covers these food and things like that we have sponsors, or other things. So

Mike Lesiecki
I'll make sure to put a link to that in the show notes. All right. All right. So

John Sands
the first thing we want to do is talk about, you know, why do we think cybersecurity needs to be taught across multiple disciplines? Well, I think most people can relate to most of these things. If you're teaching other disciplines. The first thing is the interconnectedness of modern systems. I don't care what type of discipline you're teaching today, whether it's healthcare, business, automotive, manufacturing, basically, across a myriad of different industries. Everything today is interconnected through the internet and through automation, and that's going to become even greater as AI integrates into more disciplines, and so on. And when we do that, we just naturally expose those systems to potential threats, and vulnerabilities. And what we need to do is make sure that our workforce understands it. So if we're taking health care systems, and we're interconnecting them to intelligent databases, and automation and things like that, they naturally are going to have threats to those to those systems. And part of what we like to do is as those things are being taught, and how those systems work, and, and are being used, we also want to talk about the precautions and the safety that's necessary in implementing and operating those systems. So it really is a two phase approach. It's looking at the information technology aspect of it and the operational technology aspect of it. But the two of those have expanded the need to have the majority of our workforce have to have some foundational understanding of how to keep those systems safe and what the threats are to those systems necessary. Are they growing threats, we have seen that everything from nation states to many of the organizations that have implemented ransomware attacks have really found areas that they know are going to disrupt organizations. So we need to protect those links. So you know, threats like ransomware and you know, as the world of IoT expands, and those end devices of smart end devices are really vulnerable unless people understand how to secure those those systems. And it's gonna continue everything from you know, social engineering and phishing attacks supply chain is now critically dependent on cybersecurity protection. We've already talked a little bit about AI. Part of what we try to do is let people understand this whole concept of advanced persistent threats, that if your organization is targeted by a nation state or by a group that's looking to profit, there are some really scary tools and scary technologies that they have available to them. And without some basic understanding of what those threats are, and how to countermeasure use countermeasures to protect against those threats, we really leave ourselves very vulnerable. And you we could go on and on with zero day exploits. And now things in the cloud, a lot of cloud based services, increase the vulnerability, excuse

Mike Lesiecki
me for interrupting, I don't know what a zero day exploit is. So a zero day

exploit Basically, most systems are covered by some type of intrusion detection systems or antivirus systems, things like that, right? zero day exploits basically, are new exploits that these systems are not aware of. So how do we protect against, you know, new types of threats, new signatures of these threats, and so on. And we basically talk about the tools and resources that are out there to help

organizations do that. And people within those organizations that run those systems, and maintain those systems, and so on, how they can keep up to date on things like zero day exploits and methods of protecting against those things. And then, of course, we have, you know, insider threats, AI, now, the misuse of AI is really something that's starting to scare this community, and that we've taken many steps now to to work with federal agencies and others, to protect against misuse of AI systems. And then again, traditional things like data breaches and privacy violations. You know, as we start to collect and share more and more information, it's our responsibility to keep that information safe. And that's, you know, really part of what we do and in teaching cybersecurity skills across the curriculum. And then you can see other other things like phishing and you know, nation state attacks, crypto related threats, these are just a myriad of types of things that we need to be aware of and that are growing as we automate and interconnect our systems. Recent impact of attacks, I can tell you, one of the things that really scares the cybersecurity community are some of the recent attacks that we've seen. So now we have these things called Hunter worms that will look for a target. And there are many examples of this in there, they're being paired up with things like ransomware. So we need to have people understand what these are and how to identify them, and then how to protect against them. But the point about these recent attacks, is they're no longer just attacking your data, they're now ability now the ability to take over controls and attack the physical plants and the safety of employees. So you know, it's risen to another level that really brings a lot of concern to people across a myriad of industries. And that could be everything from automotive to energy generation, transportation, I think most people have seen how each of these industry have become more and more automated and depend on on interconnectivity. And you know, the, the attackers understand that then part of is just our ethical responsibility of keeping our customer's systems and their information safe. So every organization, whether it's in healthcare, business, manufacturing, and so on has of these responsibilities. And then one of the things that I really liked to talk about is that we've gone into the next phase of cybersecurity over the last seven, eight years. In the early years, all we were worried about was taking action to protect these systems. But today, business is bringing us to another level and the federal government is bringing us to another another level with expanded regulation and compliance. So as an example, if you haven't heard of the CMMC program, it's the Cybersecurity Maturity Model compliance program. And this is just one example. But the Department of Defense and through congressional action now is going to require all contractors and subcontractors, which basically consists of over 350,000, companies now that provide services and products for the Department of Defense, by 2025, are going to have to go through a cybersecurity compliance program. And basically what consists of is that they implement certain things from a national framework. But more importantly, that they can prove that they've implemented these things and that they are effective. But this is going to become part of everyday operation, and it's gonna become part of more and more contracts. So to qualify even to qualify for a federal contract, an organization is going to have to be able to meet and then pass the these audits and they talked about it being a maturity model. What's going to happen is that you're going to start at one level, and then expectations are going to be that you go to the next level and then you go to the next level and then ultimately we get to a level that we can trust. Our supply chain is fully compliant. and protected. But there are many examples of these types of programs out there today. But it's one of the reasons that individuals across the workforce in different industries have to have an understanding this because they become part of that audit, they need to understand what are the mechanisms? What are the procedures? How do these things protect our organization, and part of a security audit is just as interviewing individuals that have to work with these systems and have responsibilities for these

systems. So that's a big area. And I can tell you more and more schools have asked us can you help us with this are there are things you can help us prepare our students for this? And can you also share content that we can work with our local businesses and helping them prepare, so they don't lose contracts, and they stay competitive within with these department defense contracts. And then finally, future workforce needs and demands. Part of what's happened in cybersecurity just like other industries, it is evolving, and the type of skills and the depth of skill are increasing. And in the past, you know, a typical worker might need to have some, some fairly, you know, simple understanding of systems. But as time has gone on, we were finding that people like operators, and people that maintain systems have to have a deeper understanding now, because when you're doing things like software updates, someone needs to be responsible to find out what vulnerabilities come with those updates, who's tested them, things like that source, and so on. So those are the reasons why, and I'm spending most of the time this morning talking about why because I think that's the biggest hurdle we have to get over is that, you know, people in other disciplines, you know, ask, How can we do this? We've already got a curriculum that's jam packed, how can we add more content? Well, these are reasons you know why we feel it's absolutely critical that we do make room and we do try to build content that can be easily adapted into our existing content to teach some of these things. So when we start to talk about multi disciplinary cybersecurity education, we really talk about it in two phases. So we talk about operational technologies. And this is the use of information systems to increase the efficiency and productivity of an organization's operations. These technologies do things like detect or control through the direct monitoring, they adore control of industrial equipment, assets, information, processes, and so on. You know, many times, the cybersecurity individuals don't have these responsibilities, they have to work with other people across the plant, or across the organization to protect these things. Most of the time, traditionally, cybersecurity people have fallen into the IT, you know, aspect, the information technology aspect. But many job roles will require knowledge beyond just traditional skills and abilities. In fact, top candidates should have knowledge of both operational technologies, and the threats and risks that accompany these these technologies. So incorporating some of these things in your curriculum will actually help better prepare your students. And you know, just as an example, just an understanding of what CMMC is all about, will definitely help your students when they apply to a organization that's going through CMMC requirements, for them to come in with an understanding of that already would be a real benefit to organizations that are that are looking to hire people that they're going to perform these these tasks. So I mean, I can tell you, we've worked across multiple programs in our institution and several of our partner institutions. And we've actually had many of the Department of Defense contractors come to us and say, Can you advertise this to our partners in our other organizations, because we really need people that can come in and hit the ground running and understand the program, understand things like the framework and so on, whether or not they work in cybersecurity, or they are maintenance technicians, or, or operators or whatever. So things like that, I think also are going to help your your candidates in qualifying for many of these jobs in the future.

Mike Lesiecki
John have you seen this as a maybe on an interview question or a job announcement knowledge of CMMC preferred or

not only have I seen it, we've actually had companies in our local area come to us and ask us, you know, where are these things taught which programs are important? And can we work with your faculty in discussing how they might want to incorporate it within some of these other programs? You know, I'm looking at specifically like manufacturing. We have a lot of our manufacturers now that really like to see all of our manufacturing students go through at least a primer of what this is all about and how it's implemented within an organization. So I think the other thing that we like to talk about when we're talking to a others about cybersecurity across multiple disciplines is that the federal government did a massive investment in trying to define what cybersecurity requirements are, what the workforce looks like. And you might have heard of NICE, which is the National Initiative for Cyber Education. So it was run by NIST National Institute of Standards and Technology. And basically what they did is a help businesses across the nation as well, as well as federal agencies define what cybersecurity work looks like. And they created this thing called the cybersecurity workforce framework. And what they did is they broke it down into seven categories. So there's seven different types of major work that's done in cybersecurity. And it starts with analysis, collection and operation of information. A whole other areas is investigation, you know, if an attack has occurred, who investigates it? How do we track that information down? How do we collect the evidence? How do we engage law enforcement things like that, to operate and maintain, operate and maintain is the area that most crosses other disciplines, because this is all about operating and maintaining our organization's operations, basically, and then oversee and govern, protect and defend and securely provision. And I think a lot of people overlook this security provision basically means large organizations have to have people that are involved in the purchasing of new systems and equipment, implementation of new systems, things like that, that they understand the vulnerabilities and the threats that go along with those things. And there's training that's involved with that, you know, it truly is a cross disciplinary area, because not only do you need to understand the threats, but you need to understand what that equipment does and how it works and things like that. So that's just one example of an area that that really has to be cross disciplinary.

Mike Lesiecki
John, for technicians, if they mostly are in that operate and maintain area, aren't they or do they cross over into some of the others, most

John Sands
technicians would would fall into three major categories operating maintain would be the largest, of course, it is the largest area within the workforce itself, by the way, then I would say the second would be protected, defend it. And believe it or not, a lot of people that are involved in protecting defend aren't necessarily cybersecurity professionals, but they are people that have the responsibility for that system, or that area of the organization. And they need to understand how to protect their resources and assets. And that's really what that was all about. So it's not necessarily that they have to have a deep knowledge of the of the tools and things that are used by cybersecurity professionals, but they need to understand the threats. And the steps that can be implemented need to be incorporated in preparing people that perform these these tasks. But they went further and he they get into 32 specialization areas. And then believe it or not, they defined 52 different work roles. Now, this is what mystifying. The department events has their own, and they defined 59 different work roles. So these are different work roles, each one of them incorporating cybersecurity. And the thing I need to make clear is that that doesn't mean all of these people go through a cybersecurity program, they may go through a

maintenance program, or an electricians program or whatever. But they have a responsibility within the organization of protecting those assets against cyber threats.

Mike Lesiecki
John, you're scaring me with all of these 52 different work roles? I'm getting nervous

John Sands
here. Yeah. And I can tell you, the framework actually makes me feel more comfortable, because it's helping organizations better understand how to protect themselves. So I think it's actually a good thing. It is complicated. But it's helping organizations better fit workers for their responsibilities in their roles, and in the most important thing, that type of competencies that they're going to need coming out of school. And that's what we're gonna we try to work with with individual schools is looking at these work roles, how do they align to your different programs? And then how can we incorporate some of these competencies that are going to be necessary to protect our organizations and our systems in the future? So this one I just show, just to show the complexity

Mike Lesiecki
of this one later. Yeah. So what this is, believe

it or not, these are all the cybersecurity industry recognized certifications that are out there today. And by the way, this grows every day. So there's new certifications that come out every day. And this is a really hard thing for someone to grasp. But basically, the way this works is at the bottom of the level, our entry level base skills that everyone needs to know about right? And as we work our way up, they become much more advanced, much more specialized, and in many cases require many more credentials, so they may require a backup For a degree and several years of experience, and so on, so works from bottom up from entry level to advanced. And then it works from left to right to the areas of, of expertise. And by the way, I don't have the whole chart here, because you would never be able to read it, right. But you can see we have very specialized areas in cybersecurity. So everything from the people that are responsible for security management, to architecture, designing the systems, and by the way, architecture is not just cybersecurity, architecture has to be built into this to the operation and architecture of the systems that design the systems themselves. So if that's a program, it has to be in, in the coding of the systems, the interface is things like that, to the analyst, to the people that have to, you know, look for what are the growing threats, and how do we modify our operations, procedures, and so on to to meet those threats, to defensive operations, to offensive operations, offensive operations, is not to say we're going out and in attacking others, but what we're trying to do is gather intelligence, so that we have early warnings, and we better understand our systems, so we can let others know about that. So, um, there's several federal agencies or organizations can work with today, in what they do is they work together nationally. So let's say if a bank on the East Coast is is just experienced a certain type of attack, we can let everyone else know about that, right. And that's what these are really all about is and when we talk about offensive operations, even to things like we put technologies out there called honeypots, which are these juicy targets that we want people to go after? So we can see what kind of tools, what approaches, what types of tactics are they using when you're going after our systems, and then we can turn that around and help different industries. A good

example, this is the is the energy systems, we've we've had several of these systems set up and it's helped us nationally protect our energy systems. So we see what you know, some of the nation states and others have tried to do in trying to disrupt energy production. Now we can take steps and we know what those methods are. And we can take better steps to protecting those things, all the way into engineering. And there's many different aspects of engineering. But this isn't a full chart. But just to give you an idea, this is the complexity of cybersecurity in today's industry. So when we talk about, you know, jobs of the future, these are the jobs of the future. And these are going to, you know, provide tons of opportunities for our students. And the thing that makes me really happy as a community college teacher, is that we looked at the seven categories of work. And this asks us to do a limited study of community colleges. So we did a study a couple years ago, we took 12 of the leading cybersecurity programs in the country at community colleges. And we track their graduates five to seven years out after graduating the programs. And basically, what we did is we had them self report, what areas of specializations they were working in, what work roles they had, and so on. And our perception of what a community college student would be five years afterwards, and where they were, were totally different. We thought that, you know, most of our students would fall into three categories I mentioned. Right, so operating, defend, and so on. Right? What we found is that many of our students work across all seven. And out of the 52 work roles, we covered 47 of the different work roles. So these are graduates of community college programs. Now, of course, some of them have gone on and finished, you know, advanced degrees and so on. But they started at a community college. And what we found is that they they really are meeting about 90% of those jobs, which was really sort of surprising to us. And then the other thing that we found is that what happened with many of these students is they were cross trained. So you know, they might have been a manufacturing the manufacturing program, but they took courses in cyber, they took courses in IT or, or maybe even coding right today. So the manufacturer might need to know how to do some some programming or scripting. And those students rise to the top of things that we would really have thought only you know, baccalaureate or graduate degrees would have been a combination of community college programs that really prepared them to take on some of them advanced

Mike Lesiecki
work roles. That sounds like a fascinating study. Well, first, it's not easy tracking for our graduates over five to seven years. So number one, did you publish that can I put a link

John Sands
on our website so if you go to and I can share the link

Mike Lesiecki
with you I'll put it in the show notes stone, they can find it there. Yeah, but you'll

John Sands
you'll see they're very popular community colleges, um, you'll recognize the name of the community colleges are some of the larger committee colleges in the country in then what we did is we we partnered with some universities and had their PhD students help us do the research, you know, again, we took 12 colleges and then we looked at 25 to 30 graduates of each one of those programs, and then contacted them and had them self assess what they were doing some of them we even dug a little

deeper because we were we were really just surprised that they were working in things like investigations and you know, some things that you think only Baccalaureate graduates with governance, you know, so yeah, cool. So, you know, we talk about challenges and barriers, we understand that you only have students for so many hours in a two year program. So how do we best incorporate these things? And how do we be able to fit them into a associate degree programs? And we spend a lot of time working on that? And then how do we prepare our faculty with knowledge and credentials to teach some of these things? And then are there instructional content that's out there that engages students in not just, you know, showing PowerPoints, but are examples,and are there exercises that students can take the things that they're learning in a current classroom and expand upon to teach some of the cyber content and that's really what we've done as a center is to try to produce a lot of those types of things. And then can we create instructional content that addresses the competencies that our businesses are asking for, or that are the credentials that our businesses are asking for? So those are some of the things that that we heard that from the community, and at our CYAD conference that we specifically address. So here are some of the things that we that we've done. So we've created very short little snippets. And we we have, we've had, we've run a faculty development National Academy for the last 20 some years. But over the last four or five years at NYcTE, what we've done is every summer, we've run these smaller programs in a multidisciplinary fashion to bring together people from across multiple disciplines, and teach them how to use some of these lessons and some of this content within their existing programs. In fact, part of the program is we help them design it, to incorporate it, where it might fit best, and what exercises might work best, or in some cases, even customize some of this content and match what they're currently teaching in the classes. And that would include things like case studies, we most of the content that we create, is highly engaged, engaging their animations, in many cases, or their simulations that students can actually, you know, run through an actual example of a specific industry and a specific concept that we're trying to teach. And then the other thing is it there are extracurricular type of activities that students can get involved with, there are many different types of, of students skills competitions that incorporate some of these things. And then the last thing, I think most important thing is the idea of building learning communities so that we bring our manufacturing and our electronics and our, our IT, our computer science faculty together to design the lessons that incorporate some of this content and where it fits most appropriately. And in many cases, you know, as we do curriculum and program updates, that they incorporate these things, and that they engage their, you know, their local business advisory committees, and you know, the idea of bringing learning communities together, I think it's been one of the things that's helped us the most. So we have our computer science faculty, we have our information technology, our manufacturing, and so on. And we have a advisory committee that we bring each of these members of the learning community to our advisory committees. And I think it's made a big difference. So these are just the resources that we'd like to share with you. So I'll give you a list of of URLs where you can reach these things. But our biggest thing is we have what we call EMATES, these are animated lessons that are on my myemates dot org, there's currently over 140 of these, but they're not just cybersecurity. There are math, there are some of these are in basic science. Some of these are in you know basic mechanics and things. So what we've tried to do is, is incorporate these things, so that if a student needs these math, math concepts to understand this cybersecurity concept that we sort of packaged them together. And what we found in many cases is people coming from other disciplines saying, you know, I could use that anyhow, scientific notation. I've taught that for years, this is a great way to teach scientific notation or engineering notation, or factoring or things like that. Right. So they're

not only help us in providing instructional content for cybersecurity, but they probably add to existing curriculum in other areas. I really good examples like logic and logic gates. We have teammates out there now to teach basic logic gates, but then we show how that's used in cryptography, and so on. So whether it's on a program and a PLC, or, you know, piece of machinery that needs understand logic, they can use that content for that as well as how to protect that system then with encryption. There's games that we've created. One of the unique things that we're working on right now is a 2D 3D environment. So we started this off by basically using it to teach career orientation. So you know, how do we bring someone into a secure environment and let them see what cybersecurity people do. So we have a full 3D environment and challenge that students can go through. But now we're expanding that. So this year, we're going to bring one out about cyber ethics. And we're going to start to do some on other areas of cybersecurity, like cryptography, incident response, things like that. And you might want to see the approach that we've taken, because I know that there's, you know, interest in using these technologies in other disciplines, embedding AI, lots of opportunity for embedding AI. In fact, we're gonna have a course on that this summer, through our academy. And then we have a virtual lab environment that we share with with other institutions, they may only be using five of our labs, but this way, they have real equipment in a real cloud that's protected, that they can use in teaching some of these concepts. And then finally, we have a series of case studies that are available to the faculty

Mike Lesiecki
members. Excuse me for interrupting John, could you expand on what embedded AI means? Are you talking about Chat CBT? Are you talking about AI that's now being used and some automation technology to better manage things? Or what does that mean, embedded AI? So

John Sands
what embedded AI is, how can we embed AI systems within the operation and maintenance of our systems, so we can do a better job of things like threat analysis, you know, we can better predict a big, you know, challenges, even things like change management, when we change things within an organization? How, what are the best ways to let people know about that? And what are the best ways that we can take steps to ensure that that doesn't interrupt our our operations, and that really falls under cyber, believe it or not, so? Okay. Um, so these are just examples of, of libraries. So you can see in here, we teach everything from blockchain and basic cybersecurity what a digital signature is. Some of these things, you know, your technicians are having to deal with them. Now, to RSA, like I said, engineering notation, but you can see these are the categories. And each month, we have new ones that are out there. So we have a large library of cybersecurity, we have a sub library and cryptography. We talked about CMMC, what that was all about, right? Well, we have emails in there to teach the framework, and how CMMC should be incorporated with it with another curriculum. And there's actually content and lessons that you could use within your within your programs to networking, programming, mathematics, even electronics. So those are examples of what's in our library, then we love to use other technologies. So if you if you've used crpytool, we've created a whole library of exercises in cryptool, that basically teach us how to protect systems using cryptography. Alright, the other ones are things like Packet Tracer, which is a simulation tool that we use. And then there, there are other online simulators and tools that we share within our environment. And it really starts with, you know, how many faculty members sign up for our summer programs are all they're all free. And when they take a class with us, they get access to these to these resources. We show them how to use them. And then,

of course, part of what we've been doing is developing more games and trying to gamify some of these things. So we work with Purdue University and others in a in creating simple games to teach concepts and to reinforce understanding of these concepts. Yeah, so action items. First thing I would do is encourage you to look into the CyAD conference. Again, it will be in Chicago this year, June 13. And we can share the link with you. It's a really good time to get together with others, and we break up by discipline. And then we work in groups of cross discipline. But it's a two way conversation. We share all of these resources as part of it. And I can tell you that people that left last year, I had many conversations about them telling me how they've incorporated the things that they took back with them from the conference last year into their curriculum this year, or they took them back to their advisory committees as they're looking at updating and making modifications to their existing programs. Because you will be able to sit down with people in manufacturing in automotive and other areas and see the things that they're doing across the country. So there's good examples of what other schools are doing and how they're incorporating these within their programs. So that's a little bit about what's happening at the NYcTE center and in what we're doing to help schools, specifically community colleges, and incorporating cybersecurity across the curriculum. And I'd be more than happy to field any questions if you'd like to email them to me. And I would encourage you to go to our website and look at faculty development opportunities this summer, and then the vast array of resources that are available to you if you're interested in incorporating some of these things. Now,

Mike Lesiecki
John, we really appreciate the offer and although the tremendous amount of resources out there just amazing for some of the things you've talked about. But one of the elephants in the room and you alluded to it is, how do you bring this stuff into your existing programs? Right? How do you shoehorn it in? Well, I liked your idea of putting in small amounts, not trying to change things like, replace courses, but rather to integrate things. It's interesting recently, I was at an advisory board meeting for an electronics program. And, you know, we got the good, strong feedback from industry. And then we said, Do you have any suggestions about what we might remove from our program? You know, to make way you know what their answer is? No, we don't have any suggestions about that. That's your problem? Well, they didn't exactly say that. But but it is a problem, isn't it? Of, of how do you make room for this? I don't know if there's a magic answer here.

John Sands
And there really isn't. I can tell you, though, I work specifically with our automotive program as an example, you know, one of the things that they had to do was to start teaching wireless technologies in that program. Because you bring a car in today, you literally plug a dongle in and you connect to that car through Wi Fi connection. And then you then see what's available on that bus and all the vulnerabilities and other types of of ways that connect to that car. So when we design that lesson on how we're going to teach wireless technologies, we threaded cybersecurity into each one of them. So you know, we introduce Bluetooth, and then here are some of the vulnerabilities, things that a technician needs to be available. Be aware of. We talked about the internet in the wireless cellular connections to the car. Again, we incorporated it there. And then we talked about smart modules within the car, which I didn't even know these existed that tell the car to report back to the dealership that something needs maintenance or replacement or whatever. What are the vulnerabilities and what are the threats that we need to be aware with with those things as well. And what I found really interesting

is our automotive instructor said, Yeah, you know, the dealerships told us we should teach this and the I didn't understand what they meant by certain things. Now I do and now that we've taught, you know, some some of these basic concepts, and you you've covered some of these things with us, and they take they've taken from there, I've never had to step foot back in one of their classes, they now basically teach those lessons. In fact, they've, they've probably taken it to another level only because that's what their advisory committee members are asking for. So, you know, and as far as what kind of things you cut out? It, it's tough. I mean, because we they wouldn't be in there if we didn't think they should have been in there. But I think our advisory committees in when they talk about competencies, we spent a lot of time today, you know, in our advisory committees talking about, you know, what are the ultimate competencies that someone needs to leave this program with? I think we got to keep our eye on that, more than the individual knowledge units or, or skills that someone comes out with the bigger competencies that are more important, some of the things they're going to pick up along the way, you know, so Alright,

Mike Lesiecki
well, John, just perfect. I'm fascinated today, I learned so much just talking to you. And and I think this whole cyber area, just, it's the essence of a cross disciplinary, how it fits in to all of the things that you've talked about today. So we're very pleased to have that as an example for

John Sands
us. Yeah, thanks. Thanks for inviting me. And, you know, again, it's important, it's important not just to us in academia, but it really is important to us as a nation, to keep our system safe and to keep our workforce, you know, knowledgeable to make sure we don't experience the types of breaches that we've seen in the past.

Mike Lesiecki
Well, you know, at our website, John preparing technicians.org. We also have some tools and resources, there's a paper on this framework approach to the cross disciplinary core. We have instructional cards that our brief learning activities, it's not exactly like the emails, but in some ways, they're very complimentary to the emails that you talked about. And we have a podcast series that features cutting edge industry interviews, as well. And we have a number of webinars like this one, John, that are recorded in our series that we like to share. Here's an example of some of those instructional activity cards. I mean, just looking at the very first column on our data knowledge, we have activities on data visualization, using spreadsheets, analytical tools, things like that. So I invite people to check out those resources. Here's an example of the podcasts and you know, the one right in the middle John episode 37 Kristine Christiensen, who talked about how they work together at your college to integrate from the business side and the manufacturing side and the electronic side a very fascinating\ podcast. We enjoyed having her hand her colleague on board, and again recordings of this webinar series are at preparing technicians.org slash webinars and additional professional development resources are available on that site plus all of the different resources that you listed today, John, so thank you. That concludes our presentation, folks. John, thank you again.