Cybersecurity in Education: Changing Behaviors & Awareness – Part 1 of 2

Jared Heiner: Welcome to another episode of Aspirations in Education podcast, brought to you by Cisco. This is your host, Jared Heiner. I'm once again excited to be presenting. I'm on with Dave Versocki, who is the Chief Technology Officer for the Capital Region BOCES in New York. He oversees, in a lot of ways, the number of different programs and the operations of the northeast information center. I also have on with me Don Harple, who is the Information Security Manager.

And today, fellas, what I'd really like to do is get into what you're working on around cybersecurity because it is a hot topic. In fact, just the last two days, I was watching the news and cybersecurity issues are coming up everywhere. And, obviously, just the disruption that it brings, the fact that there are bad actors, as we like to say, out there. I know that student information is hugely valuable from the perspective of they have untouched credit scores. And so, we can dive into all of that.

But, again, welcome. And, Dave, tell us a little bit about yourself and your role. And, probably helpful, is to tell us a little bit about the Capital Region BOCES and how it interplays with the Northeast Regional Information Center and the charge that both of those organizations have.

David Versocki: Well, I mean, for myself, I'm the Chief Technology Officer, as you mentioned, for Capital Region BOCES. I've been with BOCES in the regional information center for nine years. Formerly, a math teacher, district technology director, and have been in education since 1990. So, I've been around a little bit in the world of education.

As far as what the Capital Region BOCES and/or the Regional Information Center's roles are in life here in New York State, we are here to provide supports so that schools, essentially, can focus on the education of our children. So, when you start thinking about what that means, it ranges from everything, from providing back office supports in the business office to providing training for teachers.

In the case of the Regional Information Center, our charge is to provide all those technical supports, whether it be the hosting and management of student information systems, financial systems. And

some of what we're going to talk about today, it's the maintaining, and care, and feeding of the regional network infrastructure and the local district infrastructures. The focus today will be on what we're doing as an emerging set of services in the area of cybersecurity from a mitigation and protection standpoint and also from an assessment standpoint.

JH: And, obviously, in this day and age it's a huge, huge task. And I would assume we can give them a little bit more into this that, again, because I've worked with a number of other states who don't have these types of Regional Information Centers and that type of setup. And it's got to be hugely helpful to have a team that, essentially, is sitting there waiting to provide the service, and we can dig into that.

But I would like to welcome Don. Thank you for joining us. Can you tell us a little bit about your role, which I know has morphed? You've had a lot of different experiences. But security is, I think, where your heart lies. Tell us a little bit about your role and what you're seeing with the school districts that you work with.

Don Harple: Hi, Jared. Yeah. So, Don Harple here, Information Security Manager at the Northeastern Regional Information Center with Capital Region BOCES. So, I have had a lot of varied roles. But, generally speaking, I've been kind of the security guy for years since I started, it's been about twelve-and-a-half years here. And I've always looked at this role as really a bridge builder because security is kind of the glue which pulls things together. And I'm really excited because we're moving down a path where we can start really putting our best foot forward to work to protect that sensitive data you're talking about.

JH: No doubt. And there is quite a bit of it, obviously, in education. So, the NERIC provides support immediately to its 136 component districts. Meaning, they have the ability to access your services, but you can also expand out if their districts or RICs or BOCES that are also saying, "Hey, we don't offer this. There's a way to secure that as well." But in terms of providing this service, can you tell us a little bit about, not only the service itself, but really where the seed started to grow. At what point did you say, "Hey, we need to offer something." So, again, what are the services that you provide on top of how did this come to be and what does it look like as a package?

The Security Services Capital Region BOCES Provides to Districts to Protect Them Against Today's Vast Attack Surface

DV: Sure. Well, specific to security, it's not like security, we woke up one day and said, "Oh, we should do security." We've been doing security at the network level forever. In the days of old, it was everybody's got a firewall. So, an endpoint protection type of software and that was it. And it was pretty simple.

As you mentioned, in your opening remarks, the threat vectors out there today are much greater than they ever were. The bad actors are much bolder than ever before. And it's a business, quite frankly. It's not because somebody just wants to have fun, they're in it to make money. And so, there's a real dark business out there that it's not targeted specifically at schools, it's banks, it's our industry, it's boats, it's anything. You read it recently in the news, everybody's fair game to be a victim.

So, with that said, I think the formalization of these services was born or at least became more critical, certainly, as the regulations to once they started to be formalized and put out there. The range of services from the training and education of your data privacy officers was out there. What we call the multi-legged stool of security, which has been, for us from a security operations perspective, your firewall, your DNS level protections, your endpoint protection, some of your email layers of security that need to be had.

Those have been now formalized from, instead of, say, a la carte to now, yes, there are set of things that can be bought individually. But it's now going to be more about the aggregation of the logs and the events being created from those tools so that we can be proactive or at least less reactive in helping districts limit the exposures that they have. Don, do you want to add on to that?

DH: Yeah. So, I think the other thing to remember is that this is about layers. This is about defense-in-depth. All those buzzwords you hear about security, it's really where our heads are at. We're really focused on figuring out how we're going to create a comprehensive platform for districts to consume and protect the data. So, when you think about how does an attack start? How do they get in? Primarily, it's going to be from a phishing attack. I mean, it's the number one vector and so it starts there, but it doesn't stop there.

And the reality is, we have to do better. We have to do more. And schools don't have the capability or capacity to do this on their own. So, enter NERIC and Capital Region BOCES with, "Here, we're going to help you build out your posture and security by offering this suite of tools to add those layers to your district network."

DV: Jared, what Don just said about districts and their resources, listen, a school district's function in life is to educate students. They are not going to have multiple security people, and these systems and the

expertise to manage all these things. And so, your question was, what made us do this? Well, it's exactly that. Districts are limited in their abilities and their time, quite frankly. There's lots of smart people out there, but their time is limited. There's usually one or two key people in a district. They can't do all this stuff by themselves.

And even the Regional Information Center isn't doing it all by themselves. There are partnerships that go along with our services or behind our services, I should say. So, it's not just a defense in depth from a product standpoint. It's multiple layers of people and supports in place. And the actions that are taken that are going to make that.

Changing Behavior and Awareness of Where Threats Come From

JH: I think there's something that keeps coming, and I know this we're talking very much about the service. But, Dave, you hit the nail on the head, you said a couple of things. And, Don, you were echoing this. And I'm hearing you say, one, schools, they really need to focus on education and learning. But cybersecurity, let's be honest - what was it? - there's a gas line that just got hacked, the entire meatpacking industry. I mean this is all within the last seven, eight days.

I think we've morphed past the time where I can say, as someone in the district, "I've got this". Because to your point, there's not enough staff. I mean, when we're talking about cybersecurity, you really need to have a team of people. And we see this from an industry perspective, yet there seems to be something that says, "Hey, you know what? It's my information." Help me understand what can you provide? I know there's a service, but there's got to be a fear that says, "Hey, wait a second. This is mine." And there's all these fiefdoms inside of education, and one of them is IT.

So, what's the benefit to this program in the sense that you can say, "No, no, no. We're just providing you -" and Don used the term "-layers." How do I make sure it's customizable or it feels like mine? What are the things that I can effectively turn around and say, "Now, I have this that's specific to me"?

DV: Well, Jared, remember that the goal is not things. It's not the tools. What we're trying to change is behaviors and the awareness of where the threats are coming from. The tools are just part of the toolkit, if you would, that can reduce your risk. I think that the message needs to be, "Look, yes, at a local level, you will be involved in deploying something, of course. And you will have dashboards of certain things - in our words - that come out of these systems locally." But the benefit that we provide is, certainly, scale and, hopefully, efficiencies fiscally and, again, trained people centrally. This body of

work, this is team of people, that can be educated at the highest level interacting with those partners we referred to earlier.

And then, I think there's a check and balance that has to happen as well. And we didn't touch on this yet, but the idea that you put in some tools, fine. How do you know you're behaving the right way? I think there's the other part of this, which is the assessment side of things that has to happen. And that's your risk assessments. That's your vulnerability scanning, your pen testing. We call it the hygiene test, what is our behavior and what does our hygiene posture look like?

And every school district goes through financial audits. Every board of education is involved in the audit committee. They have an audit committee that looks at the controls around the fiscal world. This is not a heavy lift for district leadership and Boards of Education to equate. This is the same exact thing. So, when you are talking about what does our behavior look like, what are your procedures? How do you test those procedures? Who tests those procedures? And you basically get graded on how you're behaving.

And a district can't say - or it doesn't matter, district, municipality, business, you can't say, "Well, we're small. And our profile, we're too small. Nobody's paying attention to us." Go and ask some of the entities that have been compromised recently. I think they'll tell you something different. So, I think we have to continue to raise awareness, talk about things like what's the soft costs of not doing anything, or the very painful cost of not doing something when your reputation is damaged, when you have private information that gets released.

So, Jared, I want to make sure we don't talk about things, and objects, and tools, because there's lots of ways to answer those questions. More about behaviors and the acknowledgement of risk that is out there--

What Are the Biggest Obstacles to Good Cybersecurity Practices in Education?

JH: And, David, an excellent point, because you do enough research which you just have to scratch the surface to find out that human error, right, wrong, or indifferent, in the sense that I didn't intend to do this, is really what leads to some of these attacks or the vulnerabilities that lead to the attacks. And so, you've identified essentially a number of things that I think, if I'm a school leader, I'm sitting there

thinking about what some of the biggest obstacles are you've come across where folks are trying to figure out what to do. What are those hang ups that they end up kind of getting stuck with --

DV: Well, yeah, good question, Jared. Some of it is an awareness. Just purely an awareness. Like, listen, depending on the size and staffing that you have in your own district as a leader, you may have been just reliant on your team because they're good people and we got this. And they may just not be aware to the degree of the risks that are out there. It's not intentional by anybody's fault. But say, "Yeah. We're doing A, B, or C." Well, how do you do A, B, and C? I think that's part one.

Part two is just some shared stories from some of the people who have been affected, how did they feel? Don't talk to me or Don. Talk to those leaders on how they were feeling before they were compromised and how they feel after it. They got a different perspective on life.

JH: Their eyes are open, for sure.

DV: Their eyes are open now. And just as a parallel, districts that have gone through some risk assessments get their eyes opened, thankfully, ahead of time and know that "Hey, there's a set of things we need to do to change our behaviors." And then, I think, of course, the big one on the table is there's costs. Every single thing we talked about, those tools, if you would, or services, they all have a cost. And there's a balance, how do I go into this conversation? And being told I need to spend X tens or hundred thousand dollars when I know that a fourth-grade elementary section, we got some numbers that are approaching limits and we got to decide between a teacher and a cybersecurity problem.

And if what we said was true right off the beginning, what is our purpose in life? Educate students. It's really hard to have that conversation. So, I think it's looking at the BOCES, in our case from what we're talking about, it's the partnership. A BOCES isn't a vendor. A BOCES is a partner. An educational partner. So, it's about, at least, being open for those conversations. And then, the business aspect of getting there is what we can help leadership overcome. We can't make it go away. We can't make it go away, but we can help people get there.

Cybersecurity Partners Save Time and Protect Valuable Assets

DH: That's our charge. So, as a cooperative, our goal is to figure out how to do some of these things that are either time expensive, or people expensive, or tool expensive, and bring them together in a less expensive fashion so that districts can consume them in a way that they would never otherwise be able

to consume. And the reality is that it's not going to get any easier. So, I mean, now more than ever, we need to push and make sure that we can give them as much as they're going to get in a comprehensive package.

And that really relies on strategic partnerships, so we're doing everything in our power to basically aggregate the suite of things, which is more than just tools. There are people. There are other organizations who come to the table when the chips are down, and it's make-it-or-break-it time. And we've got data on the line.

Using Cybersecurity Analytics to Make Informed Decisions

JH: So, it almost sounds like we're talking about two different pillars. And, Dave, you're talking about kind of this tool before. But there's almost a, yes, there has to be some type of technology involved. But there's also kind of the awareness piece, we've talked about that. And then, I think that there's also something to be said for the analytics and this idea that we now have positions out there, security analysts. So, it's not I can plug something in and feel good. I can have a session with my staff and feel good. But at the end of the day, tell me a little bit about collecting the information and making informed decisions. I think that goes by the wayside very quickly.

DV: Well, I think there's two answers to your question. Number one, in New York State, we have some requirements for retention of certain pieces of information. I believe it's called LDS-1 -

DH: LGS-1.

DV: LGS. Thank you. LGS-1 - thank you, Don - that tells us how long we're supposed to keep certain types of logs. In this case, six years. And in who's going to be able to do that? And now, it's not just collecting it and keeping it. To your point, Jared, what do you do to analyze it and look at it? Well, that's what a log aggregation tool and/or the SIM, which is the additional component of it that will help do the alerting and the intelligence aspect, and then even taking action if you so choose to automate some of those processes. So, again, who has these skill sets and the time to go do that individually? And that's where somebody centrally could do this, and we are doing it along with a partner.

DH: But if you look at the industry, too, the industry is going in this fashion as well. Not any one security analyst or technician anywhere is doing one specific thing. So, using that mindset, we can survive in this world doing or trying to do all of it ourselves.

Thank you for joining us for PART ONE of this two-part series on Cybersecurity in Education. Please join us for part two by heading over to head over to AspireTransforms.com under the Resources tab and select the Digital Aspirations Podcasts.

Aspire Technology Partners is a Cisco Gold Certified Partner engrained in solution pillars that set us apart as a true Cisco solutions provider. We are committed to the continuous improvement of expertise and skillsets around Cisco initiatives that enable us to help and guide customers in the adoption and management of technology architectures designed to transform their organization. We hold Cisco Master Specializations in Collaboration, Security, Cloud & Managed Services and is one of only 25 partners in the US to receive the Cisco Advanced Customer Experience Specialization.