EWA Radio: When Schools Get Hacked

Originally aired Nov. 30, 2020

Emily Richmond: [00:00:09.56] This is EWR Radio, the official podcast of the Education Writers Association, and I'm public editor Emily Richmond. Increasingly aggressive hackers are breaking into school district computer systems and holding sensitive student information for ransom. In some cases, districts are paying hundreds of thousands of dollars to regain [00:00:30.00] control of their networks.

Tawnell Hobbs of the Wall Street Journal is paying close attention to this growing national trend, and it's taking on even more significance given how reliant districts have become on remote learning amid the Covid-19 pandemic. Tawnell, welcome back to EWR Radio.

Tawnell Hobbs: [00:00:48.56] Oh, hello. Thanks for having me.

Emily Richmond: [00:00:50.69] Well, let's start at the top. What kind of data are we talking about that schools are storing about students and potentially their families?

Tawnell Hobbs: [00:00:59.19] You know, it's a [00:01:00.00] lot of data. It's Social Security numbers, addresses, date of birth, court documents, and – this kind of surprised me when I saw this in the dark web – court documents for foster kids, custody arrangements.

Of course, grades. Hackers are taking grades too, which can be pretty embarrassing depending. And then also discipline records, information on children with disabilities. And I even noticed at some of the private schools, they were actually taking [00:01:30.00] income tax filings, which I guess parents admit it. Maybe they wanted to receive some help with tuition or something. So it's literally everything

Emily Richmond: [00:01:39.81] You used the phrase just now. You said you saw it on the dark web. Explain that.

Tawnell Hobbs: [00:01:44.76] Oh, God. Basically getting on the dark web, it's different websites, search engines and everything else. It almost looks like how you would go on your laptop and you put it up in those windows.

Well, when I go into the dark web, it looks [00:02:00.00] just like windows, but it's literally a dark street, and it has all the icons and everything. When you get into the dark web, like I say, it's a collection of websites, but it actually allows you to look and see what the hackers are up to.

There are actually some hackers that probably most of the ones, at least the ones that I follow, that you could only access their websites and their blogs. If you are in the dark web and [00:02:30.00] going into the dark web, it's you know, you could kind of remain anonymous. You know, I think it does scramble your IP address or something. So you can be kind of anonymous there. And that's kind of why the hackers live in the dark web.

Emily Richmond: [00:02:44.37] What are hackers doing with this data?

Tawnell Hobbs: [00:02:47.37] Oh, well, first I want to grab it because they want to use it to extort the school districts. It's like if you don't pay us, guess what? We have all of your data. We have your Social Security numbers. [00:03:00.00] We have everything. And we will actually put that out there. And a lot of it's free for the taking. You don't have to pay.

Most times you can go on there. You can just see it. There it is. Or they might sell it too. I've had some – what they call – I know a couple of reformed hackers, and they tell me, they said, sometimes for young children, their private information is like gold to a hacker because you have their Social Security number. You have their date of birth.

I mean, [00:03:30.00] about time that that child found out that their identity had been stolen, it's likely that maybe they're 16 or 17 trying to get a car or job or doing a credit check. So look how many years you have if you take a kindergartener's identity. It's going to likely be many years before it's even found out.

Emily Richmond: [00:03:49.89] This is very fascinating. And I'm wondering – how are districts protecting their data? I mean, how hard are the hackers having to work to get this? Is it like a smash and grab job, or are we talking about like Ocean's Eleven where they have [00:04:00.00] to plan for months and months to get in there?

Tawnell Hobbs: [00:04:03.09] So typically, they've already been in your system for days or weeks when they make their presence known. About time you get to work and you open up that laptop and it says your files have been encrypted, they've already been in there for a while, grabbing things typically in the middle of the night when school districts aren't around.

That's the thing about school districts and the security of their systems. They typically don't have 24/7security setup to monitor their servers. [00:04:30.00] So a lot of hackers do attack then in the middle of the night, but they're in there for days and weeks. About time they do let the district know, “Hey, we've encrypted your files,” they've already grabbed a lot of data at that point.

Emily Richmond: [00:04:46.86] What do we know about these hackers and how they choose the districts they want to target? Is it about how much cash these districts might have on hand or really more about the vulnerability of their systems?

Tawnell Hobbs: [00:04:57.72] You know, that's interesting because one of the hackers that I [00:05:00.00] dealt with, the [...] hacker, I asked that specific question, and this is a direct quote: When I asked, how do you choose your targets, your districts?

This hacker said, “High revenue and low cybersecurity is basically an open invitation.”

So they're looking at high revenue — and districts, a lot of their reserve funds and all that stuff is right there, public information. And they're looking at low cybersecurity.

And he said it's like an open invitation for [00:05:30.00] them. When the University of California, San Francisco, got hacked a few months ago, I actually saw that negotiation transcript between the university and the hacker. And the university had said that it really couldn't afford to pay a $3 million dollar ransom. And the hacker came back immediately and responded with the university's revenue for the year. And it's like, “Yeah, you can't afford it.” So that's just how it is now.

As far as like, I think what they would look [00:06:00.00] for when it comes to vulnerability or revenue there — Obviously, if you're vulnerable, they're going to get you right then and there. And then when they determine the ransom, it's going to be based off what they think you can afford.

Emily Richmond: [00:06:12.83] Do you have any idea how often this was happening before the pandemic?

Tawnell Hobbs: [00:06:16.85] You know, it was happening before, but what's different this school year and the reason why I want to highlight it is that the hackers have gotten so much more ruthless with school districts. It used to be for school districts, they would lock up the servers, you [00:06:30.00] know, make life pretty horrible trying to get you to pay. But now, they're grabbing this personal information, and they've proven that they will post it online if you don't pay. So that's the big difference under the pandemic with the school year.

Emily Richmond: [00:06:44.57] And that's what happened in Clark County, the nation's fifth largest school district, which you reported there was a ransomware hack earlier this fall. You broke [00:06:52.58] that story. How did it land on your desk?

Tawnell Hobbs: [00:06:55.16] Well, what happened was – I was already working on the story, the front page story that [00:07:00.00] ran last week, on ransomware. We're looking at the whole big picture.

So as I was working on that story, one of my sources – He is always on the dark web, and he said, “Hey, I know you're working on this big story, but you should know that this hacker just uploaded all of the files that they have on the Clark County School District.”

And this is before I was even in the dark web. I mean, this is what I really kind of decided I needed to be in the dark web. And [00:07:30.00] once he told me that and I started walking through what was in there and everything. And that's pretty much how we broke that story. We felt that that was big enough where we needed to go ahead and break that story. And I would still do the front page story. But it was interesting because the school district hadn't yet informed people in the community that their information now was living on the dark web.

Emily Richmond: [00:07:55.79] So this feels like a student data privacy failure, but also a bit of a PR failure.

Tawnell Hobbs: [00:08:01.55] Yeah, and that's what's kind of surprising to how many districts don't tell. You know, or even if they tell initially, “Oh, we've been hacked,” they won't follow up and say, “Oh, yeah, by the way, all your information is in the dark web.”

What typically happens – and here's what I will do – as soon as I see a district's information pop up in the dark web and I know they've been hacked, I will go and look on their Facebook page, just to kind of see what they're telling the community.

A lot of times they have to check on their systems. People can't register, can't get schedules. And probably eight times out of 10, the first response is, you know, “Oh, we're having technical issues or computer issues.” Meanwhile, they're dealing with this hacking situation. So they typically aren't forthcoming about what's going on.

Emily Richmond: [00:08:48.98] So that's in the short term in terms of being outward facing with the community. But how do they avoid transparency in terms of paying off this ransom? Do they go into a closed session of the school board and treat it like some kind of confidential settlement? How do they take that money out of what's public funds and pay it?

Tawnell Hobbs: [00:09:06.47] There's a couple of ways they do that, and it depends on the amount.

Certain amounts you have to have school board approval. I have also seen districts that will go into executive session, come out, just approve to pay the ransom for an undisclosed amount, or I will see, recently, what happened is the district decided that – They had gotten their files hacked. They wanted them back. So they hired an outside company to basically negotiate with the hacker. So they paid that company $300,000. What that company will likely do is go, and you know, they might give the hacker

$200,000 and keep the rest just to get the digital key to get to the district, so they can open up their servers.

Emily Richmond: [00:09:55.22] Please tell me your next story is that company and the hackers are first cousins.

Tawnell Hobbs: [00:10:01.61] You know, that's the thing. There's people that wonder about that all the time. Right.

Emily Richmond: [00:10:08.54] I had to ask. I'm sorry.

Tawnell Hobbs: [00:10:11.96] Yeah, it would be the first one.

Emily Richmond: [00:10:14.51] But, you know, it’s a laughing matter to an extent that it's just so ludicrous, but it's not funny that districts are being left vulnerable here. It's also a little unsettling that they're being left to solve this by themselves. Where's the FBI and all of this? Where's law enforcement?

Tawnell Hobbs: [00:10:30.59] Well, and that's interesting. There is no national or official clearinghouse for these cases.

So if you get hacked, it's kind of like, “OK, what do I do?”

The FBI recommends that you tell your local FBI field office. Obviously, you don't have to. Some states, if there's a data breach, require you to report the incident. But that's if there's a data breach, and people classify that in different ways.

I have some school districts, like one school district in the story that I did last week, they have like one guy in the IT department. They got hacked and they're like, “What do we do?” Because everybody's kind of Operating in silos on this thing, and that's a big problem, and there are some U.S. Congress types that do want to get that changed. So we'll see.

Emily Richmond: [00:11:22.53] We're talking with Tawnell Hobbs at The Wall Street Journal about school districts increasingly facing ransomware attacks at the hands of hackers. Don't miss an episode of EWA Radio. You never have to. You can find us on your favorite podcast app. And thank you to everyone who is rating us on iTunes. Your support and your feedback are helping us to grow.

Now, we talked a little bit about what you found in your story. I want to talk a little bit more about how you did this. You mentioned that you went into the dark web. You also reported that you were in some chat rooms talking with some of the alleged hackers. What were the special precautions you took with your own identity, with your computer equipment and to protect yourself before you went in there?

Tawnell Hobbs: [00:12:01.10] You know, that's the thing. Because when I told the editors that I would need to go in there, they were like, “What?”

But obviously, I was going to identify who I am. I plan on going into the dark web, talking to hackers. I have to identify myself as a Wall Street Journal reporter and let them know what I'm talking about, just like I would anyone else.

So obviously, you know, I talk to the editors because it was obviously risky, not just for the company and me being in the dark web and can they see our IP address? You got these kind of questions.

But also just personally, I kind of braced for a possible personal attack. But basically what our company did, they got me setup. They got my computer setup where I could safely enter the dark web.

And basically there's programs out there that will literally scramble your IP address to help you not get hacked, although it's still a risk, obviously. And then once I got into the dark web and started talking to one hacker in particular, I reached out. Because once I got to the dark web, I could go on their sites, and I could reach out to them and say, “Hey. Can you talk to me for my story? Or, Hey, I mentioned the hack you did or whatever.”

Tawnell Hobbs: [00:13:13.23] And there was one hacker in particular I mentioned in the school district story. I reached out to the hacker. They were currently hacking a school district in North Carolina. And I had reached out, and they responded, and it went to my email basket. Obviously, any time I dealt with a hacker, I was always in the dark web.

So the hacker had emailed me, and I responded, “Hey. I'm working on this story.” I identified who I am.

And the hacker said, “I will talk to you, but you have to download the Tor browser. And that's how we will chat.”

So I have to get back with my IT guys and say, “Hey. The only way this hacker is going to deal with me is if I do this.”

And they were like, “OK, yeah, we know about that. We'll do that.”

So I got set up on there, and as soon as I downloaded that software, the hacker sent me, I guess almost like a friend request, and I accept it. And we start talking after that.

Emily Richmond: [00:14:09.24] It's kind of incredible; isn't it? I'm surprised that they would want to talk with you. Were you surprised?

Tawnell Hobbs: [00:14:15.57] Yeah, I was really surprised. In the email I sent initially, I had let them know that I was going to mention the Hayward School District hacking. And I knew that they were currently hacking. And I wanted to get their side and just kind of figure out what the ransom amount was and things like that.

And they responded to me. It was a couple of days, and it was weird because when they did respond to me, we had set up a time, and my time was like 3:00 in the morning. I figure they were probably overseas. We had about an eight-hour difference in time.

So I set my clock, got up at 3:00 in the morning. I heard nothing from them. 4:00 in the morning, nothing.

And then about 15 minutes later, it popped up, and I could see that they were on there. And I said, “Are you there?”

And they said, “Hi, we are.”

And we just start talking. We talk probably that night for about an hour through chat.

Emily Richmond: [00:15:07.64] It's really incredible. For a reporter who wants to start looking into this in their own district and obviously may not have the capability to safely start poking around in the dark Web, it would make sense to start by asking their own district some questions, right?

Tawnell Hobbs: [00:15:18.86] Yeah. And that's what you do. I mean, if you see that your district has a big technical problem one day, and everything is down. The website is probably down. Parents are saying, “Why can't we access it?” So many people are doing remote learning. There could be a good chance that they're being hacked.

And, sometimes if you ask them straight out, they'll say, “Wow, you know, how do you know?”

And sometimes I do just because I'm in the dark web, and I physically see the hacker saying, “Hey.”

What hackers will typically do is when they hack a district, if the district doesn't pay, they will put up what they call a warning file. And that file is not going to be it's not going to be the most sensitive information. It might be like a roster. And they're just proving to the district, we have your files; we have access. This is our first installment.

And at that point, if the district doesn't pay, they start uploading more. And a lot of times when school systems are down, that is what's going on.

It is kind of hard to get the school district talking. Because some of them, if they reach out to the FBI and all of a sudden I know it's kind of like a federal investigation, so they're not going to talk about it.

I'll be honest, the best way I knew what was going on with school systems, and I could actually call them and say, “I know you're being hacked. I know what you're telling your public, but I'm looking at your files right now on the dark web.”

Emily Richmond: [00:16:44.87] What do we know about the district's legal obligations to disclose this information, though? For example, if I did a FOIA request to say, “Have you anything related to ransomware or hacking?” Would they have to disclose it?

Tawnell Hobbs: [00:16:57.41] It depends, or it depends on the state too in some cases.

Some states actually require school districts to report to the state education agency if there has been a data breach.

Now, anybody would say, once a hacker enters your system, that should be a data breach. Some people disagree with that.

Some states that don't have it, you could fire the school district and say, “Hey, I want information on all of any ransomware attacks or cyber attacks.”

It depends. A lot of this stuff – If it's under federal investigation or under investigation, they can reject you and say that's currently being investigated and typically they're going to win that battle.

The problem is these investigations get opened, and they stay open so long because it's really hard to catch these hackers. The ones that seem to hack these school districts are overseas. So it is difficult to get it.

The best way that I seem to get it is when they're going to pay the ransom and the school system, they need board approval or something like that. And it might be discussed in a public session.

Emily Richmond: [00:18:03.02] Well, it's a good reason to look through that packet beyond the consent agenda, definitely.

Tawnell Hobbs: [00:18:07.88] I have my tweet deck set up, and it will bring in anything, any tweet or press release or whatever, dealing with problems with district computer systems.

And typically it's a parent saying, “Why can't we register? Is the system going to be down all day?” That's typically my cue to go check around. I'll look to see if the district has said something like, “Oh, we have technical issues we're working out.”

And then typically, I'm going to the dark web next, and I'm going to see if their stuff is in there and who's hacking.

Emily Richmond: [00:18:43.53] What's been the reaction to your reporting. Have other districts come forward or officials or even hackers?

Tawnell Hobbs: [00:18:49.41] Oh, that is interesting. I've had a lot of different people come forward, not any hackers, but I've heard from employees that are in districts, especially if I mentioned them. They said, “Yes, that happened, and now my identity has been stolen.”

So I hear from people who feel like their information was compromised, and now people are trying to open up car loans in their names and things like that.

I've also heard from employees that said, “Hey, you know, we got hacked, but nobody ever wrote about it.”

And typically it's because your district didn't make it public. That's why.

Emily Richmond: [00:19:28.57] Let's talk about some story ideas for education reporters and some questions maybe they should be asking of their districts right now about data privacy. I mean, especially in this era of remote learning, when kids are online more and more and so are teachers and staff.

Tawnell Hobbs: [00:19:43.48] What I would do, first of all, I would find out in your state the law as far as reporting cyber attacks.

That would be interesting. Because like I said, I am fighting and I'm doing some of that. And I'm finding there's a lot of districts that are reporting to the state because it's a requirement, but they're not always letting the public know.

So I would find out first: What is the state requirement there? Some states don't have a requirement. OK.

But if the districts are required and then that's when you FOIA the state education agency and you say, “I want the list of all districts that reported its cyber attacks,” and you get the list that way.

And I would do that first and then you could probably start requesting documents.

But like I said, sometimes in this situation, it's really hard to get documents because everybody falls back on, “It's currently under investigation.” These things are under investigation for so long because they don't get solved.

I’m in a fight with the state right now over that. And that's kind of their whole world. You know, “We told you the names, but we don't want to give up anything else because there's all these investigations going on.”

Tawnell Hobbs: [00:20:49.03] So I would definitely find that. Also, what I found that was really interesting in some of these attacks is the length of time that districts keep personal information.

I felt I had reached out to one lady that I had come across. It was like her adoption record. I mean, literally, it had everything in there from sexual abuse and everything else. And I had reached out to let her know, “Hey, you know, you've been compromised. Did you attend this school district?”

And she's like, “Yeah, but I graduated like seven years ago.”

So there's some cyber experts that believe that they don't know why districts keep personal information like that on file for so long, especially when they don't always have secured servers.

And what happens with some of this old data, old information, it gets pushed back to some old server that nobody really thinks about anymore. Those are the least secure servers to hit.

So it would be interesting to figure out what is the rate in which those files are cleaned out in those school districts. I think a lot of the hacks I see, the hackers are able to go back at least five years into old information.

Emily Richmond: [00:22:00.58] I think what's interesting to me is what are districts doing to prepare staff to be the first responders here and to maintain those firewalls, like what extra training is being provided, including just like awareness about phishing scams? — which, as you mentioned, is just one way that the hackers get in that open door.

Tawnell Hobbs: [00:22:17.38] That would actually be another good story idea to find out what your district is doing to make people aware.

I have seen districts that are trying to educate kids on what not to open. Do a little test about, “OK, would you open that? Yes or no?”

I've been told a majority of these hackers get in through these phishing scams where they send you an email. I got one today. I mean, it looked like a real official company email, but I knew it wasn't.

And it's like click here to look at your whatever. So I noticed that some districts are spending the money, spend the time to educate staff and students. Because, mind you, there's a lot of kids with laptops, a lot of kids getting on the system. You know, that's a lot more entry points. Right.

So a lot of them are trying to educate. Well, some of them anyway, are trying to educate staff and students. But that's probably a good thing to look at, too, in your district. How are they prepared for the possibility of some kind of cyber attack?

Emily Richmond: [00:23:18.38] Ok, now tell me the truth. How fun was this story to report?

Tawnell Hobbs: [00:23:24.26] You know, I got to tell you. I had a horrible experience. I thought they had come after me. And here's why. Any time I had a computer issue, I thought it was one of the hackers. There was one instance where I had done a story about the hackers attacking some election files or something. Right.

Because I was in the dark web and I saw that this county elections office was being hacked. So we end up doing a story off of it.

So I had just filed that story. I think it had just posted. And I remember I got a call from one of the editors, and he's like, “This is weird. Your bio has disappeared.”

This is the bio you can click on to see my name or my stories and you could see my bio and past stories or whatever.

And of course, I immediately get on the laptop and start calling up all of my colleagues and all of their bios were there.

Tawnell Hobbs: [00:24:22.79] And I'm like, oh, shoot, the hackers are coming after me. Maybe.

So I got my editor and of course, she's on high alert, and we all are because everybody knows what I'm doing: This project and who I'm reaching out to.

And it was just me. I've been here for years and never did I have a problem with anything computer related.

So they got the IT department involved, and they were like, “This is strange.”

So I said, “I'm working on this story. I'm dealing with these hackers, and I just want to make sure they're not trying to send me a warning.

And then they figured … for some reason, a period was missing in the URL And so that got fixed. I still to this day, don't know, because these people are very savvy. They are good.

And even my company, we took precautions, but they knew there was a possibility that they would be able to get in. You know, no matter all the precautions we took, there was still that fear that they would come after us.

Emily Richmond: [00:25:18.68] So I think that would be what the closing advice would be to the other reporters who are out there right now, which is if you're going to proceed on this, proceed with caution and proceed with editorial support.

Tawnell Hobbs: [00:25:28.16] Yes, there's just no way I would have felt comfortable corresponding with a hacker without safeguards in place because my IP address is out there and just everything. So that was a fear.

And also, like I said, and my company did talk to me about this, they obviously could come after you personally, too. So that's something obviously to think about. But, you know, I kind of weighed everything, and there was no doubt I was going to tell the story because I felt that it needed to be told, and everybody needed to know.

And maybe districts will see that and say, “Oh, we're not alone. We're not operating in a silo.”

And districts learn from each other. And maybe it gets attention to where, you know, like I said, those to U.S. Congress folks. They actually did start making some moves just to get it addressed because it is a big problem in districts.

You know, a lot of them are cash strapped, and here they are dealing with the cyber attacker in the dark web, someplace that they didn't think they'd ever have to go.

Emily Richmond: [00:26:27.16] Education reporters learn from each other, too. And we really appreciate you taking the time to share your expertise with EWA radio.

Tawnell Hobbs: [00:26:33.89] Oh, you're welcome. It was enjoyable. Thank you so much,

Emily Richmond: [00:26:37.31] Tawnell Hobbs is the national K-12 education reporter for The Wall Street Journal. She has spent more than 17 years covering education issues and joined the Journal. In 2016. She joined EWA Radio from her home office in the Dallas bureau. Thanks again Tawnell.

Tawnell Hobbs: [00:26:52.49] You're welcome. Thanks for having me.

Emily Richmond: [00:26:56.47] And that wraps up another episode for us. If there's a story or a reporter you want to learn more about, drop us a line.

We're at ewaradio@ewa.org.

The mission of the Education Writers Association is to strengthen the community of education journalists and improve the quality of education coverage.

For more than 70 years, EWA has helped reporters get the story right. Have a great week. Take care of yourself and thanks for listening.