MPR News | Minnesota Now Expert: Cyberattacks on local governments are no longer rare
01KPP07AM8C9VEN187P5TPEHTP

NINA MOINI: Two recent cyber attacks have highlighted the risk that hackers pose to local governments. Last week, Spring Lake Park School District canceled school for two days after its technology team learned an outside actor had infiltrated its system. A week before that, Winona County took its systems offline in response to its second cyber attack this year. The first was in January. So both Spring Lake Park schools and Winona County said they were working with law enforcement and cybersecurity consultants to try to understand what happened. Cyber attacks are becoming more common and more advanced.

According to the state's information technology agency, MNIT, each attack that forces systems offline brings this issue to the surface again. But my next guest thinks about it all the time. Faisal Kaleem is Director of Cybersecurity and Cyber Operations Programs at Metro State University. Thank you so much for joining the program again, Faisal.

FAISAL KALEEM: Hello, Nina. Thank you very much for having me on the show.

NINA MOINI: This is so important and we're so happy to have your expertise around all of this. It does seem like we're hearing about this more and more as it pertains to local governments. What was your reaction to hearing about these most recent attacks?

FAISAL KALEEM: Very simple. These attacks are no longer rare or sophisticated outliers. They are routine, targeted disruptions of local government, especially the one that lack the resources to defend themselves.

NINA MOINI: Well, and when you talk about those resources to defend yourselves, I feel like a lot of the people I talk with at the county or city level are talking a lot about how outdated a lot of their software and systems are. I mean, to your knowledge, do a lot of people have what it takes to defend against something like this?

FAISAL KALEEM: I don't think so. I mean, again, this is where the lack of resources comes in. If you remember a few months ago, the St. Paul attack, I mean, if a resourceful city like St. Paul can be brought down, imagine these smaller cities and counties and school districts-- they don't have enough resources to defend themselves.

NINA MOINI: So I have here that local governments and contractors reported 269 cybersecurity incidents to the state between December of 2024 and November 2025, this past November. That averages to about five incidents a week. Can you describe the range of what this might look like? I think people think, how will this directly impact me? We saw in the city of St. Paul, it took a while to get people to be able to pay their bills and to access things. But what is the range that you see in these types of attacks?

FAISAL KALEEM: A range-- there are so many different statistics out there. The numbers that you are talking about sounds accurate. But the problem right now is the reason why you are having these sharp increases, because ransomware-- which is a very common attack-- has now become a common business model. And these criminal groups, they now sell tools and services.

So I mean again, for your listener, there is a terminology we use called ransomware as a service, which means that you don't need to be highly technical to launch these kind of attacks. You can simply rent these kind of tools from underground websites or these criminal groups who sell these tools. And then anybody is able to launch these attacks. So this is the reason why this is becoming so scary. And again, local governments are attractive targets, as I mentioned, because they provide essential services but often lack those enterprise-level defenses.

NINA MOINI: To your knowledge, what groups-- I mean, you're saying it doesn't really take that much sophistication anymore, and we don't know sometimes who or what organization or group might have been behind something like this, or even just an individual. Are you getting the sense that it is more individual or more of coordinated attacks?

FAISAL KALEEM: So we learned that when it comes to the St. Paul, there was a group by the name Interlock that actually attacked the St. Paul city. So far, there is no attribution of the attack when it comes to Winona and the school district. But when we talk about these groups, they're what we call a super-syndicates as well.

They are major ransomware, as-a-service groups are forming alliances to share infrastructure. For example, Scattered lab source, basically they call them f lab source hunters or the LockBit, Qilin, DragonForce Alliance. Like, there are a bunch of these alliances which basically are at the super syndicate level. But then again, as I mentioned that there are some low-key groups as well who basically look for these opportunities to try to extort some ransomware.

NINA MOINI: So based on the numbers we talked about, five of these types of incidents a week or on average, they're not making the news. But I'm not hearing about five of these a week. And then I'm listening to a lot of news. Is there a point where a local government has an obligation to reveal that something like this has happened, that an outsider has gotten into its systems? Are they required to immediately report this, or does it have to reach a threshold of impacting constituents?

FAISAL KALEEM: Well, as a matter of fact, effective December 1, 2024, I think there is a Minnesota cybersecurity legislation that focuses on a strict incident reporting for public entities and enhance consumer data privacy. I mean, again, they did it because they want to enhance the whole consumer data privacy. So when it comes to these incidents, again, as I said, as of December 1, 2024, public agencies and schools must report any cyber incidents to the MNIT, or a "MNIT" within 72 hours.

And then obviously, the Minnesota Consumer Data Privacy Act grants residents, starting in 2025-2026 rights over their data, including access, deletion, and opt-outs for targeting advertising. So again, there is now this formal incident-reporting law that was enacted, which means that they must report any sort of incident within 72 hours.

But on the other hand, I would also tell you that sometimes, some of these incidents do not get reported because they are so scared of the reputational loss. They feel like that, hey, if we report these issues, there is going to be big deal when it comes to their reputation. So that is the reason sometimes they decided not to report. But again, they are obligated now, as far as the public entities are concerned.

NINA MOINI: They're concerned about losing the confidence of the people that they're meant to serve?

FAISAL KALEEM: Exactly.

NINA MOINI: I do wonder about artificial intelligence, something that a lot of us are trying to wrap our heads around and understand. Does AI have a role in maybe some of these attacks, but also in cyber defense?

FAISAL KALEEM: Oh big time. I mean, AI, when it comes to the cyber attacks, what's changing right now is that AI is accelerating both sides of cybersecurity-- the attackers and the defenders. And again, the scary thing is, for example, the new models like the Anthropic's Mythos, or Mythos, that shows just how fast this is evolving. So I'm not sure if your listener heard about this thing. This actually made quite a news a few weeks ago. What Mythos actually can do.

I mean, this is an advanced AI model designed to find software vulnerabilities at scale. It can identify previously unknown flaws. And in some cases, it can actually generate various ways to exploit them. It is so powerful that it has not been released publicly. I mean, again, AI, from the bad actors' perspective, can definitely do worst.

Because all these phishing emails in the past, we can spot out those grammatical mistakes and all those kind of things. But my God, these AI-based phishing emails, it's so difficult to find those phishing emails. And sometimes, even for people like us, it's so difficult for us to be able to find those emails as well. But again, to your question, yes, from the defender's perspective. So all these different companies, they are also introducing some AI-based technology into their tool sets as well.

NINA MOINI: OK. So it's something that can be helpful, but is also harder to keep up with and moving rapidly? Just lastly, Faisal, I mean, as we're talking, I am feeling like I'm curious to know what you would recommend to some of these school districts, cities, counties who maybe feel like they don't have the resources or the money to begin to adequately defend against something like this. Where would you tell them to start? What is something attainable that you think that some of these smaller entities can do to try to protect themselves and the people they serve?

FAISAL KALEEM: Absolutely. Obviously, there are some basic things that they can follow. I mean, we always talk about the basic cyber hygiene that includes a strong password, multi-factor authentication. We talk about backing up the contents all the time. We talk about making sure that their softwares remains up to date-- patched as soon as the patches are available.

But on the other hand, Nina, I'm going to do a shameless plug over here. Because what we are not thinking as a state is some shared responsibilities and some shared services. So, for example, Metro State Applied Innovation Institute, we basically have some very good services, for example, our cybersecurity clinic. And I really encourage anybody who's listening right now-- even if it's a school or if it's a county or city or if it's a small business-- we can provide free-risk assessment services to you guys under our cybersecurity clinic.

From the technical perspective, we actually have implemented two security operations centers. One is on campus where our students are going to sit down and monitor the university networks. And we encourage our university partners as well to let us monitor their network. But on the other hand, we also have an external security operations center that was funded through a small business grant, and the purpose of that security operation center is to provide 24/7 monitoring to all these under-resourced entities.

And again, we are talking about low cost or no cost, because we have some grant money. We can use some grant money to provide some 24/7 monitoring services. So the very first thing, obviously is that they need to get these kind of monitoring services. I mean, gone are those days when you are living in the reactive-- I mean, they're still in the reactive model. We have to think about this thing on a proactive basis. So again, we can help them. But again individually cyber hygiene, backup, and all those kind of things are the ones that they need to worry about.

NINA MOINI: Faisal, thank you so much for coming on *Minnesota Now* again and sharing about these resources. Really appreciate your time.

FAISAL KALEEM: Thank you very much, Nina. Thank you very much.

NINA MOINI: Faisal Kaleem is Director of Cybersecurity and Cyber Operations Programs at Metro State University.