Source MinnPost (2021): https://www.minnpost.com/state-government/2021/12/minnesota-has-done-well-protecting-state-agencies-from-cybersecurity-threats-a-new-legislative-commission-wants-to-keep-it-that-way/

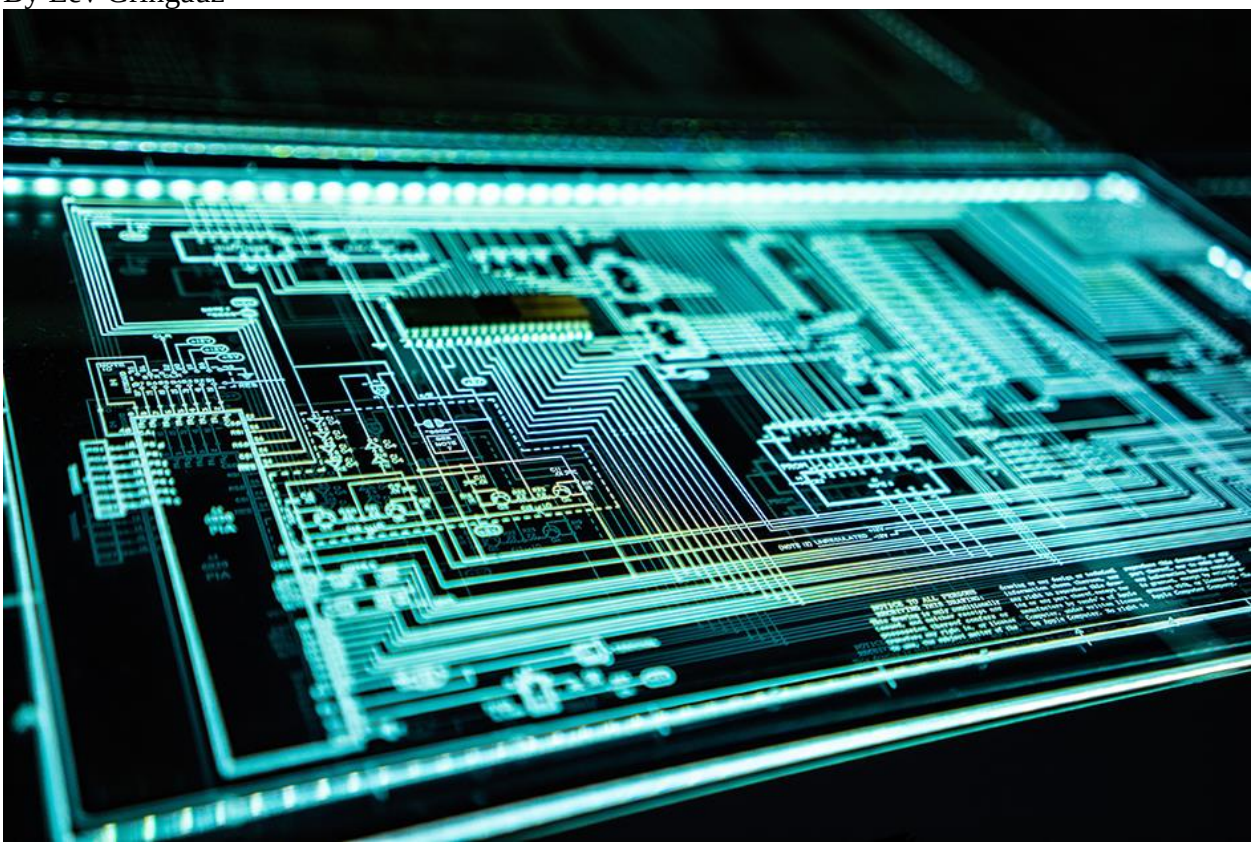
News

State Government

Minnesota has done well protecting state agencies from cybersecurity threats. A new Legislative commission wants to keep it that way.

Though Minnesota is does well in protecting state agencies against attacks, there are a lot of vulnerabilities at the local level.

By Lev Gringauz



The Internet Association, a trade organization of tech companies like Amazon and Rackspace, scored Minnesota number one in cybersecurity preparedness out of all states in 2020.

Photo by Adi Goldstein on Unsplash

Dec. 17, 2021

Every month, Minnesota IT Services (MNIT) defends against roughly 27,000 phishing emails and messages targeting employees of state agencies.

Designed to trick workers into giving up access to Minnesota's computer systems, every message is a chance for hackers to steal residents' social security numbers, their banking and health information and to shut down state services with a cyberattack.

"Those services can be as simple as renewing your driver's license or…getting access to social services, whether it's SNAP nutrition programs, or educational programming," said Rep. Kristin Bahner, DFL-Maple Grove.

So far, Minnesota has come out ahead against these digital threats. The Internet Association, a trade organization of tech companies like Amazon and Rackspace, scored Minnesota number one in cybersecurity preparedness out of all states in 2020. But for states, protection against hackers isn't guaranteed; earlier this month, the Maryland Department of Health was hit by a cyberattack that left it unable to report COVID-19 metrics.

> "The risk is, have we understood what our threat actors are doing tomorrow, what they plan to do the day after?" Rohit Tandon, chief information security officer for MNIT, said. MNIT protects 35,000 state agency employees who handle data for roughly 5.7 million Minnesotans, and provides internet services to counties, cities and universities across the state.

Rohit Tandon

Now, the state is getting help from a new Legislative Commission on Cybersecurity, created earlier this year, which will advocate for more cybersecurity resources and legislation at the Capitol. For MNIT and other government IT managers, it's is a lifeline to much-needed support. For members of the commission itself, it's a way to push other lawmakers to meet what they see as a fundamental responsibility.

"If there's such a failure where we're not protecting our citizens' data…our citizens don't have an option to go next door and shop for a different government to get their daily needs met," said Sen. Mark Koran, R-North Branch.

Counties particularly vulnerable

In 2019, the Legislature approved $20 million over the next four years for MNIT's cybersecurity efforts. Since then, no other funds have been set aside specifically for digital security. "We are working on responding…[with] a budget on a much slower cycle than those who are able to work on and devote resources to malicious attacks," said Sen. Melissa Wiklund, DFL-Bloomington.

To change that, members of the cybersecurity commission — two Republicans and two Democrats from both the House and the Senate — have to educate the other lawmakers on the state's security needs. There's a lot to cover, starting with the fact that though MNIT is doing well protecting state agencies, there are fewer success stories at the local level.

This summer, the city of Lewiston had its computers locked out by a ransomware attack. And last year, a phishing attack on South Country Health Alliance, a health plan owned by Goodhue County that serves eight other counties, exposed 66,874 members' personal health information.

Counties are particularly vulnerable to cyberattacks, said Leah Patton, executive director of the Minnesota County IT Leadership Association. Many make regular backups of their systems to be able to restore them if an attack happens, and have dedicated IT directors to look after tech needs. But a vulnerability for one county is a vulnerability to all counties.

Phishing emails are hard to stop, Patton said, because an employee might "click on a link, and then all of a sudden, that bad actor…can start emailing other counties [and gain access to their systems] because it looks like it's coming from a legitimate address in a different county."

With state services often accessed by residents through their county, a cyberattack could leave local officials unable to fulfill basic needs like tax collection or accessing health information.

As a result, any talk of cybersecurity for state systems needs to involve the counties. "We're the ones that actually log into those systems and enter our community members' data in there to get them services," Patton said.

Sorting priorities

So far, the cybersecurity commission has met twice, in November and December, and members plan to meet again in January to take a closer look at the state's security risks and draw up legislative solutions.

"Right now, there is no base level of funding that's dedicated" to cybersecurity in the state budget, Koran said, and he wants funding "on an annual basis, and to make sure that it's not a short term [solution] fighting for funding every four years."

Members of the commission also agree that cybersecurity should be declared as critical infrastructure in state statute, which would help Minnesota receive federal disaster relief funds if a successful cyberattack happens.

For local officials, the commission will streamline their efforts to explain cybersecurity needs to lawmakers. "We all of a sudden have a very specific committee that we can go to," Patton said. "Prior to that, bits and pieces were spread all over into different legislative committees, which is hard for us to keep track of and the public to actually follow."

But it may be a while until the commission's impact is felt. The Legislature will set the next state budget in 2023, which makes it unlikely that big spending bills are passed in the upcoming legislative session, leaving the legislative session next year unlikely to see many bills passed.

Minnesota is also slated to get roughly $17 million in federal money for cybersecurity efforts from the federal infrastructure bill signed by President Joe Biden, though there are few details on how the money will get to the state, or if the Legislature will have a say in how the funds are spent.

More work remains on understanding how the state can also help the private sector navigate an overwhelming barrage of cyberattacks.

“We are fortunate here in Minnesota to be home to many Fortune 500 companies,” Bahner said. “And as a matter of practice, we’re seeing more and more ransomware attacks being perpetrated…in terms of leadership and being strategic, we need to make sure that the statute and the law get ahead of some of those concerns.”