Awareness, Communication Integral to Minnesota Cybersecurity Strategic Plan

Theo Douglas | May 2, 2018

The state of Minnesota’s new five-year cybersecurity strategic plan is aimed at improving its ability to combat and neutralize bad actors, and many of its 18 overarching strategies center on including staffers in the drive to enhance cybersecurity as the agency’s first line of defense.

The state of Minnesota’s new five-year cybersecurity strategic plan is aimed at improving its ability to combat and neutralize bad actors, and many of its 18 overarching strategies center on including staffers in the drive to enhance cybersecurity as the agency’s first line of defense.

Minnesota operates what it believes to be the “broadest network” and “largest amount of bandwidth by volume” of any other state, Chief Information Security Officer Aaron Call told *Government Technology* recently, because it is an Internet service provider to schools, counties, libraries and other smaller governments as well as state-level agencies. But that, he added, creates “a pretty broad target.”

The state “secures and manages” systems in more than 1,300 locations and faces daily cyberthreats from more than 150 countries including denial of service (DOS) attacks, ransomware attacks, and direct attacks on state agencies and vendors. “On average, state systems that are accessible from the Internet are probed over 3 million times daily,” MNIT said.

“On behalf of the people of our state, we need to shore up our cybersecurity defenses against those intent on stealing our personal information or disrupting the services on which so many Minnesotans rely,” MNIT Commissioner Johanna Clyborne said in a statement.

The new strategic plan groups tactics into four categories: proactive risk management, improved situational awareness, robust crisis and incident response and partnering for success. Atop those, Call said, may be situational awareness, which he said “is typically where you want to start” in building a foundational security program.

The new strategic plan groups tactics into four categories: proactive risk management, improved situational awareness, robust crisis and incident response and partnering for success. Atop those, Call said, may be situational awareness, which he said “is typically where you want to start” in building a foundational security program.

This new plan and the state’s accomplishments in IT during the last year will help shape a new tactical plan this summer, compiling needs and strategies MNIT believes can be accomplished in the next 12 months.

Situational awareness strategies include the recommendations to detect security anomalies faster and to improve the state’s understanding of the IT environment. The latter, officials said in the plan, “will help the state security program gain a more comprehensive understanding of the business systems that it now supports,” including the hardware and software underlying each.

The CISO said enhanced situational awareness may also aid in the consolidation of executive branch IT, set in motion with passage of the 2011 IT Consolidation Act.

Proactive risk management encompasses 11 strategies, the most of any category, and includes the recommendations to conduct continuous risk assessments; improve access management — a consistent issue in state and local governments; communicate security risks to agency heads; and get “catastrophic cyber risks” coverage — essentially, cyberinsurance.

Call described communicating with agency leaders as a “force multiplier” that makes tasks at hand easier once leaders understand the risks and are “participating in managing the risk they inherently own anyway.” He said a “strong governance capability” connects the enforcement of secure baselines and improved access management, indicating these and other strategies can ease delivery of “resilient, supportable IT at scale” while highlighting anomalies, enhancing detection and remediation.

The state doesn’t have comprehensive cyberinsurance, the CISO said, though some policies may cover “very, very specific things.” But while examinations of coverage have revealed unaffordable premiums, the state will likely go back out to market later this year to gauge what’s happening. Following previous explorations, Minnesota decided instead to invest in improving existing security programs.

The theme of security education as a defense against cybercriminals is emphasized in strategies centered on partnering for success but appears elsewhere in the plan as well. Among those featuring education are recommendations to educate employees about risks, use strategic partnerships to improve security, and develop a talent feeder program with higher education.

Empowering general awareness helps all users, even those who are not security-focused or at admin levels, spot phishing attacks and avoid clicking through bogus emails, the CISO said.

It also enhances the overall culture of awareness that MNIT continues working hard to foster — not an easy task among roughly 35,000 employees across multiple organizations — but one that brings with it a spirit of innovation and forward-thinking evident in a recent agency effort.

During the last month, MNIT prevented “the use of certain email protocols that potentially could have had operational or functional impact to users,” Call said. This elicited concerns from just two of the state’s roughly 35,000 employees, and these were subsequently allayed.

During the last month, MNIT prevented “the use of certain email protocols that potentially could have had operational or functional impact to users,” Call said. This elicited concerns from just two of the state’s roughly 35,000 employees, and these were subsequently allayed.

MNIT’s strategic plan is “built around what we can do with our current resources,” the agency’s Director of Communications Cambray Crozier told *GT*. But fully addressing its 18 strategies “will require assistance from policymakers and business leaders,” the agency said in its news release. And obtaining newer, more capable tools to further the prevention of incidents like DOS attacks is correspondingly more expensive; “and so part of that strategy is, again, it’s just based upon raw dollars,” Call said.

In his 2018 Budget for a Better Minnesota, Gov. Mark Dayton proposes investing $19.7 million to minimize “risk exposure” by “ migrating business systems to upgraded, modern, secure data centers,” MNIT said. The proposal would also replace and upgrade “ unsecure” equipment, pay for the deployment of more sophisticated software to prevent attacks and fund services for “continuous security monitoring” as well as tests and audits.

With less than three weeks remaining in the current legislative session, officials are hopeful security funding may yet be approved.

“I do feel like we’ve got some support and interest, of both the governor’s office and the legislature. It’s a matter of them figuring out how to see eye-to-eye on how to actually do the funding,” Call said.

http://www.govtech.com/security/Awareness-Communication-Integral-to-Minnesota-Cybersecurity-Strategic-Plan.html