GDR Global Data Review

Arizona bill would ban taxpayer-funded ransomware payments

Ken Silva
13 January 2022

Credit: Shutterstock.com/JonManjeot

Cybersecurity experts say an Arizona proposal to ban publicly funded ransomware payments is a step in the right direction, but needs to be coupled with IT upgrades for public agencies.

Arizona representative Shawnna Bolick introduced two bills on Tuesday as state legislatures return to session. One bill aims to restrict taxpayer-funded ransomware payments, and another imposes breach reporting requirements to the director of the Arizona Department of Homeland Security.

“As more data security breaches and ransomware attacks are on the rise, we must ensure the bad actors are not receiving compensation for these breaches,” Bolick said. “The FBI does not support paying a ransom in response to a ransomware attack; neither should the state of Arizona.”

Bolick said paying ransoms don’t guarantee data retrieval, funds crime, and encourages other hackers.

“With the additional policies and reporting requirements in place, Arizona can be recognized as a top leader in this country when it comes to responding and shutting down this criminal activity,” she said.

Cybersecurity experts largely agree.

"This development out of Arizona is consistent with this nationwide push to deter ransomware attacks, and congruent with actions taken recently at the federal level," said Kristin Bryan at Squire Patton Boggs in Cleveland. "I would expect more states to take similar action this year along these lines."

Bryan noted recent US Department of Treasury actions to disrupt ransomware by sanctioning cryptocurrency exchanges and banning payments to certain networks. The Biden administration has also **removed barriers** to information sharing between public and private entities and threatened to void contracts with non-secure government contractors.

Despite this, the treasury department said in November that the $590 million in ransomware payments up to that point in 2021 already exceeded the $416 million paid across 2020 – which is why state policymakers are joining the search for policy solutions, said Bryan.

Ropes & Gray partner Edward McNicholas also said the Arizona proposal is a step in the right direction, but added that it would bring short-term pain in exchange for long-term gain. He noted that exemptions would have to be included for critical infrastructure such as hospitals.

"Arizona's proposal to ban payment of ransoms by state entities is a laudable example of the states working as the 'laboratories of democracy' to create a new approach to these vexing issues," he said. "The Arizona approach is surely the best path forward in the long run, but it will inflict near term costs on Arizona's agencies, cities, and citizens."

To limit that short-term pain, McNicholas said Arizona lawmakers would also have to overhaul their public IT systems.

"Ransomware is so effective against state and local entities because frequently IT budgets have been neglected for years in favor of keeping taxes lower," he said. "We are seeing some states reap the bitter harvest of neglecting IT modernisation spending."

Norma Krayem – the head of the data practice at lobbying firm Van Scoyoc Associates (VSA) – agreed that public entities are in desperate need of security upgrades.

"As states like Arizona contemplate possible laws to ban ransomware payments, it's critical that there is a focus on the front end to see if public agencies have the resources, tools and expertise they need to imbed cybersecurity protections at the front end," she said. "It's best to evaluate the full spectrum of the problem, including what would happen if there was a complete loss of data and systems by all state agencies in a cybersecurity attack and ransomware demand, and if public services could still be offered before making a decision to ban all ransomware payments.

However, Krayem expressed skepticism at the idea that US governments would devote enough resources to make the Arizona proposal feasible on a national level.

"Federal law enforcement and the US Department of Homeland Security have tremendous tools to help assist state, local and tribal territories in a cyberattack, but not enough resources to help all 50 states if everyone goes in this direction," she said.

Ken Silva

Author

ken.silva@globaldatareview.com