

Title: **Iowa officials outline cybersecurity strategy**  
 Author: ROD BOSHART Journal Des Moines Bureau  
 Size: 36.27 column inches  
 Sioux City, IA Circulation: 39986



# Iowa officials outline cybersecurity strategy

CIO says state is at 'moderate' risk

**ROD BOSHART**

Journal Des Moines Bureau

DES MOINES — State officials are moving forward with a coordinated strategy to beef up Iowa's efforts to combat cybersecurity attacks or threats, with a special emphasis on protecting critical infrastructure and guarding against communication breaches.

Bob Von Wolfradt, the state's chief information officer, said an initial assessment put Iowa

at "moderate" risk overall to cybersecurity threats, but he noted that "the threat is everywhere all the time," so increased vigilance, training and education are key components of the first state-wide strategy.

"By implementing the recommendations outlined in the strategy, Iowa will be better able to not only respond to cybersecurity events but also to proactively

mitigate risks for our citizens and government operations," Gov. Terry Branstad said in releasing the strategy Monday. "Cybersecurity is a top priority for Iowa."

The 36-page booklet details steps the state needs to take to increase overall "resilience" to cyberattacks, primarily focusing on "lifeline critical infrastructure" sectors — such as energy, transportation, and communication

— and state government as it relates to the protection of digital government services and citizens, the governor said.

Also, the strategy outlines recommendations in the areas of risk assessment, implementation of best practices, awareness training for state employees, public

Please see **Cybersecurity**, Page A5

## Cybersecurity

From A1

education, collaboration with the private sector and educational institutions, data-breach reporting and notification requirements, and updating Iowa's emergency response plan to specifically deal with the physical consequences of a cyberattack on the state's infrastructure.

Cybersecurity isn't an "easy" topic, Branstad said, because Iowa citizens and businesses don't want to talk about their vulnerabilities, but new technologies require more information sharing, so it's helpful to communicate what has worked in thwarting cyberattacks in private or government sectors.

The governor said he planned to use the coming

months to assess the costs and policy implications of the recommendations with plans to include possible funding and legislative initiatives in his Condition of the State message and state budget proposal that he presents next January.

"This thing is a rapidly changing environment," said Branstad. "This is an ongoing thing that we all need to work on."

Von Wolfradt said one area of emphasis is to train state employees who are entrusted with a lot of data to identify and report emails with "malicious" content they might receive but not click on to invite possible computer breaches like other states or the federal government have experienced.

"We're just trying to figure out the best way to put a

fence around that and make sure everybody coming in is understanding what the threats are out there," he said.

Mark Schouten, director of Iowa Homeland Security and Emergency Management, said an attack against Iowa's electrical, gas or water systems could cause significant damage to property, loss of life or lead to civil unrest — so it makes sense to build partnership using the state's existing emergency and hazard response plans to deal with cyber threats.

The Office of the Chief Information Officer was the lead agency in formulating the strategy with the assistance of the Iowa Department of Public Safety, Iowa Homeland Security and Emergency Management, the Iowa Communications

Network, and the Iowa National Guard.