

The Case for IT Consolidation

Louisiana is saving millions and better guarding against security threats by centralizing its information technology.

BY ELIZABETH CRISP

Elizabeth Crisp covers Louisiana politics, state government and higher education for The Advocate, which published this story on Dec. 31, 2017. Reprinted with permission.

Three years after a major overhaul of the way the state controls its information technology systems, Louisiana is saving millions of dollars, and officials say that it's well positioned to protect information from security threats.

Efforts are underway to learn even more about cybersecurity threats and what more can be done.

"Right now, I think the state is in its best posture ever, and we're continuing to improve upon that," Dustin Glover, the chief information security officer in the state's Office of Technology Services, said in a recent interview.

Governor John Bel Edwards (D), through an executive order, created a 15-member "cybersecurity commission" to identify and mitigate the state's risks.

In announcing the group, Edwards said his goal was for the state to "continue our commitment to establishing cybersecurity capabilities and resources in order to adequately maintain the stability of public services while ensuring proper privacy and protection for

Cybersecurity Task Force

The mission of the NCSL Cybersecurity Task Force is to engage members in policy discussions, to extend networking opportunities to legislative leaders through a series of programs and webinars on critical cyber policy issues and to support private-public networks. By participating in ongoing projects, NCSL members can learn best practices and develop guidelines for implementing easily replicable cybersecurity initiatives. To learn more about the task force and its strategic partners, visit nctl.org.

the data that is entrusted to the state by our citizens."

Edwards has picked Craig Spohn, executive director of the Cyber Innovation Center in Bossier City, to lead the new commission. It will be staffed under the Louisiana National Guard.

Aside from monitoring the state's security measures, part of the council's charge is to fos-

Consolidation Is Catching On

When ranking their top 10 priorities for this year, state chief information officers put consolidation of government IT services and governance at No. 3, according to a recent National Association of State Chief Information Officers survey.

Why is consolidation so important? Budget pressures and the need for greater efficiency have prompted the movement in most states. And the effort is paying off. Oklahoma's comprehensive statewide technology consolidation reportedly saved the state more than \$372 million annually. Ohio reported savings of \$50 million in just the first two years of its consolidation.

Consolidating IT resources across a state, though not an easy process, is clearly the favored path. The chief information officers association surveyed state CIOs in 2016 about the status of data-center consolidation. Forty-two percent said they had completed consolidation, 47 percent said consolidation was ongoing and 11 percent said it was planned.

Consolidation can take different forms. Some states merge physical IT offices and servers and create a single agency to serve the IT needs of all state departments. Others consolidate applications, so that agencies have the same software for common business processes such as payroll and accounting.

Another model is a federated approach, with data centers and infrastructure housed in a central IT organization, but with staff and managers remaining in each state agency or department.

Legislatures have driven consolidation in many states. Louisiana lawmakers created the Office of Technology Services in 2014. The new law authorized the state CIO to oversee operation of information technology and resources, and to coordinate all IT systems across the executive branch. It also required the CIO to report on progress to the Joint Legislative Committee on the Budget.

Minnesota passed legislation in July 2011 requiring the state to consolidate IT services. The state's IT employees now report to a central IT agency rather than individual state agencies. Legislatures in Alaska, Colorado, Hawaii, North Carolina, Oregon, Utah, Virginia and Washington, among others, have also passed laws recently to consolidate IT services or provide funding for consolidation.

IT governance structures vary, but every state has a single statewide chief information officer or equivalent in the executive branch. A state CIO provides leadership and management for a state's IT programs and works with agency CIOs and IT leaders throughout the state to support overall goals.

A growing number of states also have created the role of chief information security officer to establish, oversee and facilitate a statewide program to ensure that information is adequately protected. At least eight states—Arizona, Colorado, Florida, Kentucky, Massachusetts, Ohio, Utah and Washington—require, by statute, a statewide executive-branch CISO position or positions in state government. Other states have created CISO positions through executive orders or agency actions.

The responsibilities of the CISO include creating statewide security policies and IT standards, requiring information security plans and annual assessments or reporting, and requiring periodic security awareness training for employees. CISOs with this type of governmentwide authority are better equipped to coordinate and enforce these security measures.

—Pam Greenberg

ter cybersecurity education programs, research and jobs.

Louisiana leaders say the state is always vulnerable to cyberattacks that aim to breach or damage computers and networks. In addition to potentially costing the state money, those threats also pose privacy risks for residents.

"It's always going to be a target," Glover said.

Representative Barry Ivey (R), who often totes an iPad around the state Capitol, sponsored legislation last year requiring an overview of Louisiana's current cybersecurity measures and other information technology issues. He's on the National Conference of State Legislatures' task force on cybersecurity.



Representative
Barry Ivey
Louisiana

He said he doesn't have legislation in mind just yet, but he hopes that the report due to the Legislature next month will help identify areas where improvements can be made.

"It will help us understand where we truly are vulnerable and assess whether additional funding is needed and where the most critical needs are," Ivey said. "Understanding where the big holes are could help us prioritize the spending."

He said he worries because most breaches exploit vulnerabilities. Without knowing those potential entry points, the state is less prepared to stop threats, he said.



“We are responsible for so much personal information that we must do what is necessary to make sure it’s safe and secure,” Ivey said.

Louisiana set out on a wave of upgrading its computer systems and consolidating its information technology efforts under the executive branch in 2014. The move has been the subject of glowing articles in Forbes magazine and other business publications.

“A budget-constrained state government may be the last place you’d expect to find a top-to-bottom digital transformation that ranges from citizen-facing services all the way to the underlying network. Louisiana, however, is well on its way to such a transformation,” Forbes reported in August.

The Office of Technology Services manages an average of 585 million “events per day”—which can include someone logging into a computer, sending an email or visiting a website. There are about 40,000 users in the executive branch.

Whenever an activity is flagged, the IT team reviews the issue.

Eight issues reached the level of becoming “incidents” that had to be more thoroughly investigated in 2017, Glover said. None reached the level of becoming a breach or major issue.

“That’s where we want to be, obviously,” Glover said.

A cybersecurity report compiled by Verizon in 2017 found that public-sector entities were the third-most common breach victims, behind financial organizations and health care organizations. That report also

found that public-sector entities were most likely to be intentionally targeted.

Often threats come in the form of emails that appear to be authentic and are tailored to a state-specific function.

Glover said that attempts to click on suspicious links or open attachments are flagged by his department and evaluated before the tasks can be completed.

He said the goal is always to improve and make the system as efficient as possible. “We’re making significant strides within that regard,” he said.

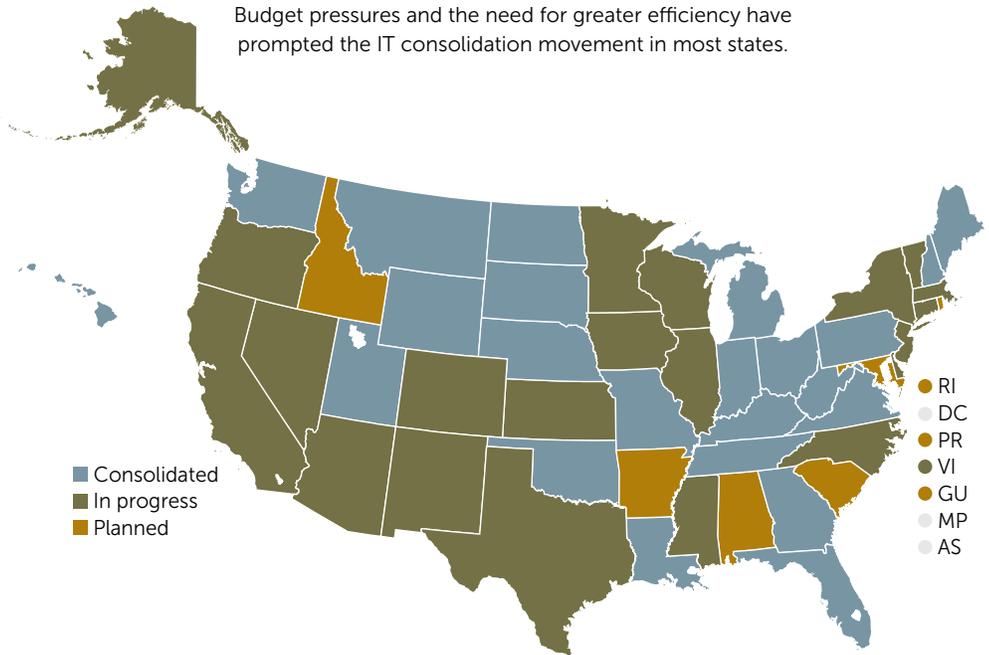
Glover said the consolidation of information technology services under the Jindal administration has helped the state modernize its efforts.

Before state agencies were moved under a centralized operation, each managed its own information technology efforts. Glover said that left holes in the system. Some smaller agencies didn’t even have a dedicated IT professional on staff full time.

The Jindal administration announced in 2015 that in the first year of the consolidation, the state saved about \$75 million on its IT services—about \$20 million of that in the general fund.

Enterprise Data Center Consolidation

Budget pressures and the need for greater efficiency have prompted the IT consolidation movement in most states.



Source: NASCIO 2016 State CIO Survey, with 2017 updates