Rhode Island Current

166 Valley St Building 6M, Suite 103
Providence, RI 02909
July 18, 2025

Dear NENPA,

As Friday news dumps go, the email we received from the office of Rhode Island Gov. Dan McKee at 6:28 p.m. on Dec. 13, 2024, was jaw dropping: The governor was holding media availability at 7:30 p.m. to announce a major cyberattack on state government.

The story kept developing over the weekend. By Monday, state officials said between 500,000 to 600,000 Rhode Islanders had their personal information stolen and likely exposed on the dark web. That number eventually rose to almost 650,000, approximately 59% of the state's population — anyone who used the RIBridges portal to enroll in the state's public benefits system or to sign up for health coverage through the state's health insurance exchange.

All major news outlets covered this story which continued well into the new year. But only one reporter, Rhode Island Current's **Alexander Castro**, dug through records publicly available on the state's procurement website for IT services. What Alex found in a 25-page request for proposals was alarming — a technical document with a diagram that showed the system architecture of RIBridges.

The schematic was meant to inform potential vendors about the system they were bidding to improve. But the document was essentially a blueprint for how the system works and the way its parts make up the whole — potentially making the system vulnerable to cyberattacks. And it had been online since September, months before the hack.

I'm nominating Alex for the high quality of his reporting and for his professionalism and commitment to protecting the public's interest behind the scenes leading up to the story's publication on Jan. 22, 2025. Rhode Island Current could have published a story days earlier but delayed publication until making sure that the sensitive information Alex found was removed and no longer available on the state's website.

Much of the blame for the data breach was focused squarely on the state's vendor, Deloitte, which created the centralized system in 2016. But Alex's reporting showed that state officials also bore responsibility for what happened.

Rhode Island Current

Alex interviewed an independent cybersecurity researcher on Jan. 8 who suggested the document he found might be a security risk. Alex then emailed state Department of Administration officials for comment on the perceived risk and received a response that the department was working on it. After catching the state's top cybersecurity official after an unrelated meeting on Jan. 17 and asking him about the document, Alex again followed up with state administration officials. They got back that night — a Friday — saying the state couldn't comment.

Alex refreshed the procurement page multiple times over the weekend until he finally saw the document had been removed by Saturday night, Jan. 18. Monday was a holiday. He returned to the story on Tuesday and found the same diagram appearing in another RFP on the state's website. Alex emailed state officials again to let them know the sensitive information was still exposed, but the diagram was still online as of midday Tuesday.

State officials replied to Alex with a thank you Tuesday afternoon. At the time, the document was still online but was removed about two hours later.

Throughout this time when the document was still publicly available, we debated whether to run the story or not. Other news outlets had already mentioned that the state had issued an RFP to modernize the system without going further into detail.

We wanted to be cautious. We were juggling other stories and wanted to give this story our full focus. So we continued to revise the story and held off publishing until Wednesday, not an easy thing to do when you are excited about journalism that holds government officials accountable. Alex and I worked together through multiple rounds of edits. I even had Alex do a last look to ensure he couldn't find the document on the website.

After the story ran, other news outlets took note, asking state officials to comment on our story at a press conference. They declined. Alex's reporting received mentions from local political columnists at WPRI-TV 12 and The Public's Radio. He was awarded a third place writing award in the Single Topic Series category for his continuing coverage of the RIBridges data breach from the Rhode Island Press Association this spring.

I hope you'll agree with me that Alex's outstanding work on this story rises to the highest levels of journalism ethics and practices and is worthy of a Publick Occurrences Award.

Thank you!
Janine L. Weisman
Editor-in-Chief
Rhode Island Current
(401) 490-1633

Rhode Island Current

RIBridges data breach stories include:

Rhode Island state government hit by major cyberattack, Dec. 13, 2024

Governor urges Rhode Islanders to take precautions to protect personal data, Dec. 14, 2024

RIBridges attack linked to Brain Cipher ransomware gang, Dec. 16, 2024, 1:41 p.m.

Many questions for Deloitte as state officials roll out response to cyberattack, Dec. 16, 2024, 8:34 p.m.

RIBridges data dump deadline may not have passed. It might be Wednesday afternoon. Dec. 17, 2024

Hackers sit on RIBridges data dump, Dec. 21, 2024

Data stolen from RIBridges shows up on dark web, Dec. 30, 2024

RIBridges has many lines of defense. How was the system breached? Jan. 10, 2025, 5 a.m.

Letters go out to RIBridges customers whose data was stolen, Jan. 10, 2025, 6:17 p.m.

Everything you need to know about RIBridges' backend was on the internet for the past six months, Jan. 22, 2025

State relaunches RIBridges portal, one phase at a time, Jan. 23, 2025

Deloitte pays $5 million to Rhode Island to cover costs of RIBridges data breach, Feb. 4, 2025

R.I. House bill would expand notification obligations after data breach, Feb. 12, 2025

After RIBridges breach, R.I. state agencies share high tech wish lists at budget hearing, April 7, 2025

Rhode Island's IT department wants a fresh install of 15 full-time roles, May 13, 2025

RIBridges firewall worked. But forensic report says hundreds of alarms went unnoticed. May 15, 2025