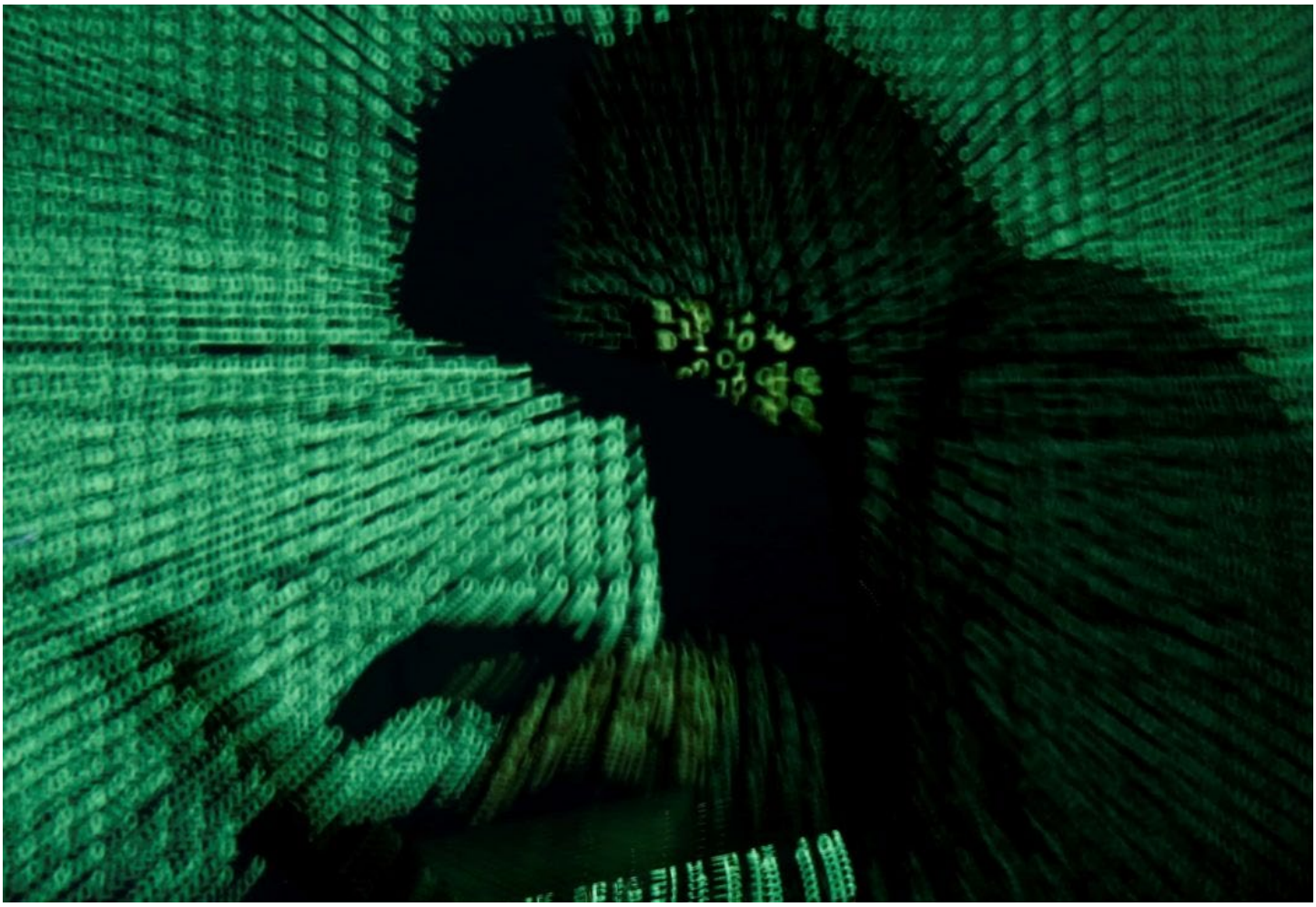
Dan's Papers

Cyber Snafu: Suffolk Ransomware Attack Ripples Across County

Timothy Bolger | October 5, 2022



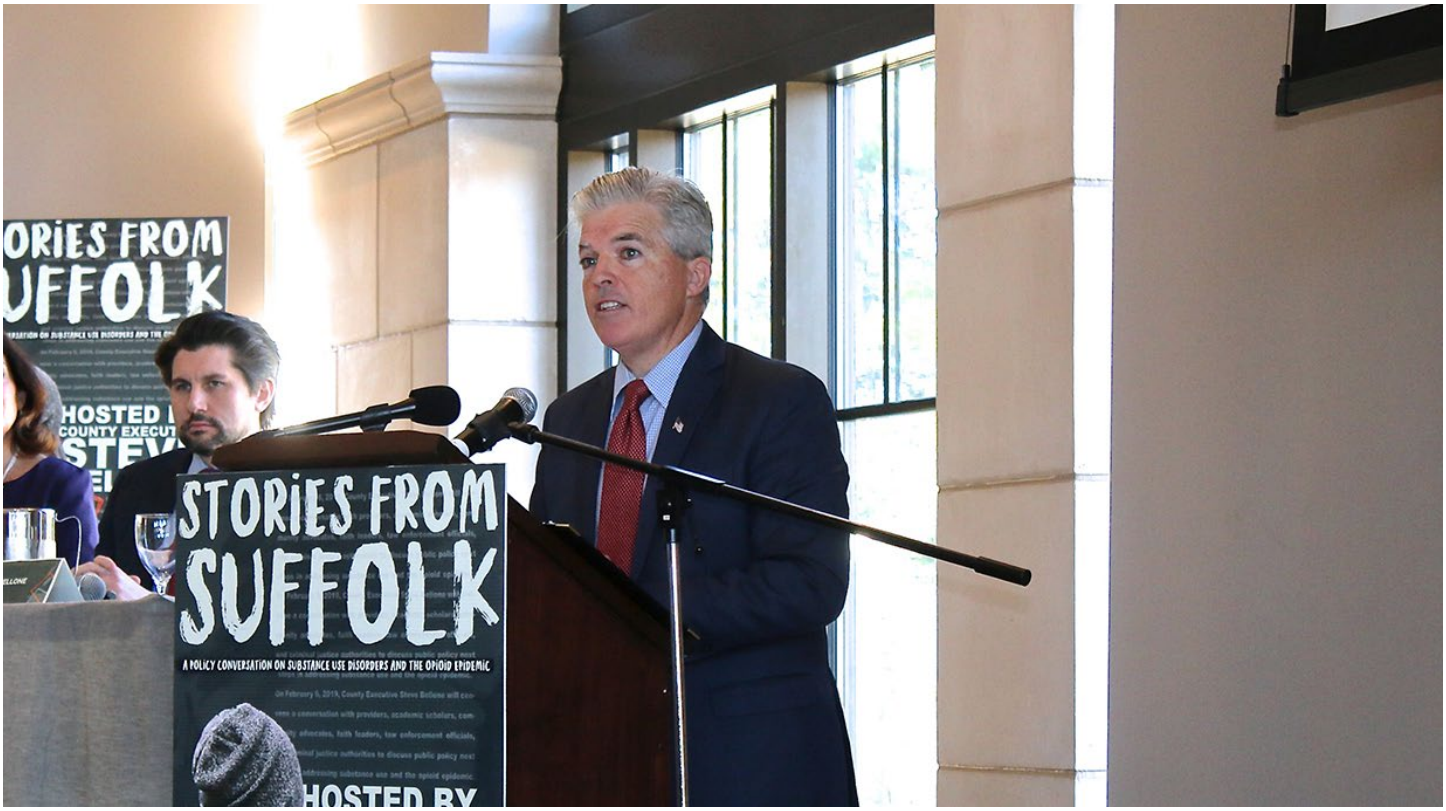
Hackers demanding ransom for the release of Suffolk County government data that the cybercriminals seized has triggered a wave of headaches for lawmakers, businesses and residents across the East End and beyond.

Suffolk officials took the county website offline on September 8 to contain the damage and started incrementally restoring access about three weeks later. Hackers claiming responsibility for the attack posted on the dark web screenshots of some of the documents stolen from county servers and later followed through on threats to release more if the county did not pay a "reward." County representatives did not answer questions about if they paid the ransom.

"We are working to ensure services that our residents rely on are restored in a safe and secure way," Suffolk County Executive Steve Bellone said in a statement.

The breach appears to be the most high-profile cyberattack ever against a government entity on Long Island. Local school districts have been the target of such attacks over the years, but the Suffolk cyberattack is the first known incident to disrupt an entire county's operations in the region. Such attacks are increasingly common nationwide.

County officials maintained that it was business as usual despite county lawmakers sharing their personal email addresses on their social media accounts to remain accessible to constituents and many county government tasks typically performed online temporarily converted to paperwork. A temporary landing page remained in place of the county website at suffolkcountyny.gov as of press time, nearly a month after the attack was discovered.



Suffolk County Executive Steve BelloneGianna Volpe

BUSINESS IMPACT

Among the industries most impacted by the cyberattack was real estate, as attorneys, brokers and title insurance providers were hamstrung by access being cut off to the county clerk's office that maintains key records required in property sales transactions.

"It was no treat being down for three weeks," said Chris Nuzzi, executive vice president and regional director of Advantage Title, a title insurance agency. "Not having access to the clerk's records made it extremely difficult to keep things in process."

East Hampton-based Town & Country Real Estate CEO Judi Desiderio said in an email that it is impacting real estate market data reports.

"The disruption is greater than I can express," she wrote. "But for the purposes of reporting on real estate closings, suffice to say these statistics — ALL statistics — are missing the last three weeks of 3rd Quarter 2022 reportings. There is no saying when the reliability of all reports will resume, since the problem remains."

The clerk's office began to resume in-person title searches at its Riverhead offices on October 1 as a part of what a county spokesperson called the "rolling restoration of services" in which "the most essential functions" are prioritized.

"The real estate industry is critical to our economy, and last week, I met with various stakeholder groups to discuss contingency plans as the county continues to assess the cyber intrusion," Bellone said of restoring access to the Suffolk County Clerk's office to allow real estate transactions to proceed.

Nuzzi said the dozens of transactions that were stalled due to access to the clerk's office records being paused had an economic impact.

“You can easily say that over the period of several weeks there are billions of dollars [of real estate transactions] that could potentially be sitting on the sidelines,” he said.

Suffolk County Sherriff’s Office at the Riverhead jail

LAW ENFORCEMENT AFFECTED

Both the Suffolk County Police Department headquarters in Yaphank and Suffolk County Sheriff’s office in Riverhead have been caught up in the cyberattack.

The hackers wrote in posts that court and sheriff’s office records were among the data seized. And the police department has had to rely on outside agencies for assistance with basic functions such as fingerprinting, background checks and more.

“While our internal process may be a little different, residents can still expect the same services they rely on,” said Derek Poppe, assistant deputy commissioner for public affairs, who noted that 911 is up and running. “The SCPD has partnered with the New York State Police to ensure a seamless continuity of services. In addition, we are doing live-scan at State Police barracks across the Island, meaning that when an arrest happens, SCPD officers process them at the NYS police barracks, including fingerprinting. Troopers are also helping members of the department with running data during traffic stops such as running plates, identifying arrest history, warrants, VIN numbers, stolen cars, etc.”

Suffolk Police Commissioner Rodney Harrison said staff from partner agencies were called in to lend assistance and there was an increase in staffing in the department’s Communications Section with the addition of 10 emergency complaint operators from the NYPD. There is also assistance being provided to the department from regional partners in coordination with the state Department of Homeland Security and Emergency Services.

A spokesman for the sheriff did not respond to a request for comment.

NEXT STEPS

The investigation is continuing into who is behind the attack and how to prevent a repeat in the future.

The attack is attributed to a type of ransomware — malicious computer code that holds web-based data hostage unless demands for payment are made — known as BlackCat. A screenshot of the purported message stated that the hackers seized 4 terabytes of data that includes files from government contracts and information on private citizens, according to DataBreaches.net, a blog that tracks such cyber incidents.

Neither the county nor the hackers' message indicated a dollar amount for the ransom that was demanded. The county hired multiple cybersecurity firms to conduct an examination and restore services. It has offered to help anyone whose personal information was publicly exposed, putting them at risk for identity theft.

"The county will notify any affected individuals as required by law, and all of those affected individuals will be offered free identity theft protection services," the county said in a statement on its interim website. "However, because the assessment is ongoing, Suffolk County wants to ensure that employees, residents and stakeholders are informed about precautionary measures they can take to help them protect themselves from becoming victims of fraud or identity theft."

If the attack will impact the county's ability to hold the elections in the coming weeks remains to be seen.