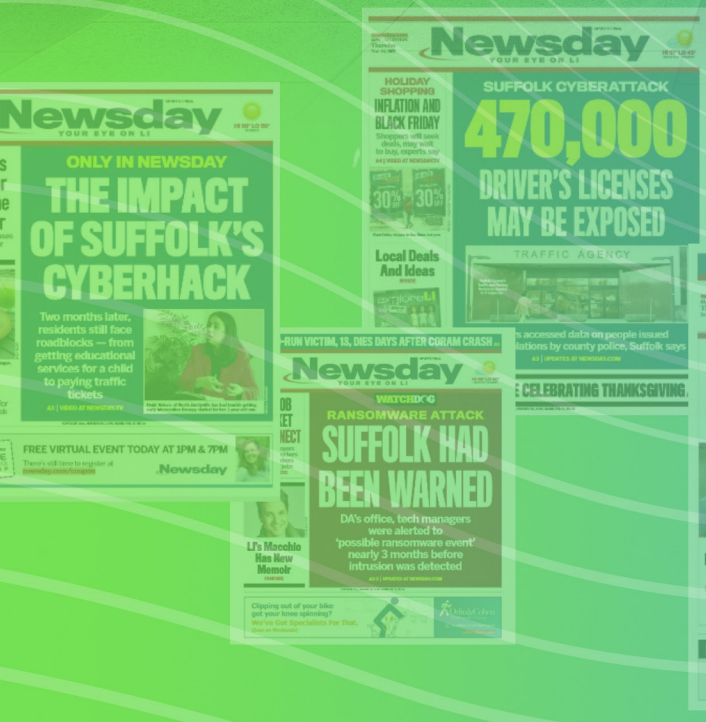
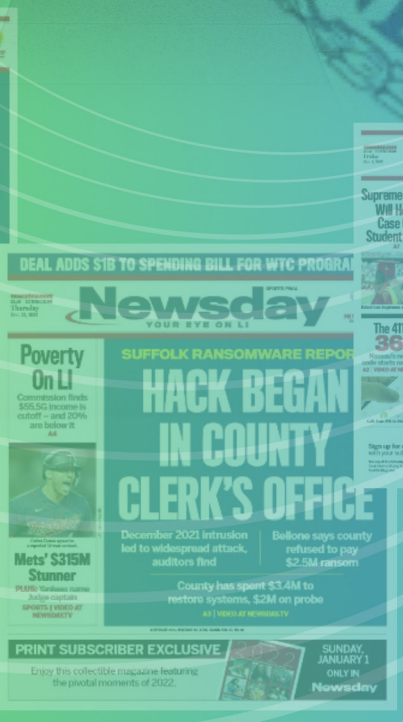
RevBits®

Suffolk County Hack Part of a Chinese Plot?





Chinese criminals linked to the communist regime were likely behind the massive September 2022 hack that froze Suffolk County's computers, according to a review by RevBits, a Long Island-based cybersecurity solution provider.

County officials ignored a series of crucial warning signs, enabling hackers to plunder sensitive county databases, stealing some 330 million pages of government information. The data stolen from county systems included 4 terabytes of confidential information, including the Social Security numbers and related identifiers of 26,000 county employees and retirees. Thieves also grabbed the confidential information on nearly half a million motorists who received traffic tickets over the previous decade. The attack was so extensive that it delayed the official tallying of votes in last year's gubernatorial race by hours.

"The failure to protect the data in a timely manner resulted from a combination of technical ineptitude and bureaucratic complacency driven by partisan political bickering."

The failure to protect the data in a timely manner resulted from a combination of technical ineptitude and bureaucratic complacency driven by partisan political bickering. The county's follow-up, substantially shielded from public view, gives no indication that leaders have yet faced up to the likely international nature of the attack.

The Suffolk cyberattack is part of an international hacking campaign

The assault on the full range of municipal government computers in the suburban county of 1.5 million people – a geographic entity bigger than all but six U.S. cities – came at the same time hackers working with or for the Beijing government began an international rampage exploiting a recently discovered software flaw. The tech world lit up with the announcements that more than 10 percent of major computer systems were at risk. While computer experts scrambled to apply patches, officials in Canada shut down the nation's Revenue Service computer system as well as computers at Metrolinx, the Toronto transit system used by 65 million passengers each year. The vulnerability also led to a crash in the email system of the Belgium Ministry of Defense, a founding member of NATO.

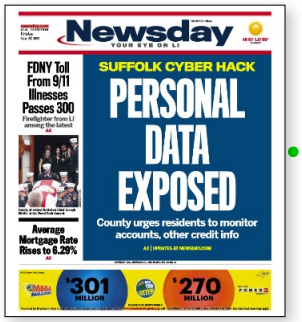
Suffolk County took no remedial action to protect its vulnerable system, ignoring not only the worldwide alert but also a specific alarm from the local District Attorney's office four months earlier.


Newsday
POSSIBLE SUFFOLK 'CYBER INTRUSION'
'OPERATING OLD SCHOOL'
County using paper after it took down computer systems in midst of cyberattack investigation
POLIO
KING'S SPEECH
GUNS
MLB

September 10, 2022


TOP STORIES
CLAIM OF RESPONSIBILITY IN HACK
Bellone: Criminals threaten to publish county documents

September 17, 2022


Newsday
SUFFOLK CYBER HACK
PERSONAL DATA EXPOSED
County urges residents to monitor accounts, other credit info
FDNY Toll From 9/11 Illnesses Passes 300
Average Mortgage Rate Rises to 6.29%
$301 MILLION
$270 MILLION

September 23, 2022

"Beyond the generally sloppy practices, the county had specific warnings they chose to ignore," said RevBits CEO David Schiffer. "There were major red flags that went unheeded while the hackers continued operating in plain sight, stealing information and expanding their illicit reach for months. All of it could have been prevented if county officials had even a basic understanding of the dangers lurking in the cyber world."

The profile of the hacking group that has emerged over recent months indicates the source as one of foreign intervention, with the attack focused more upon collecting personal information than on seeking a quick financial return through ransom or similar tactics.

On April 17, the FBI issued a statement regarding ongoing actions by Beijing to exploit stolen data. "According to statements made in April by FBI Director Christopher Wray, the Chinese government will stop at nothing to attain greater wealth and power, silence any opposition, and promote its authoritarian views around the world."

While Suffolk County's response stands out as especially naïve, the U.S. government is not well-prepared for the ongoing cyber duel with the Asian power. Wray testified in Congress last month that Chinese hackers outnumber FBI cyber investigators by 50 to 1.

Cyber threats from nation-states need greater focus and attention

News of the Suffolk attack reached the public while the U.S. government was already focused on seemingly unrelated Chinese threats. A wayward Chinese-released balloon believed to be carrying surveillance equipment and heated debates in Congress to ban popular social media app Tik Tok, for fear it provides Beijing with an unfettered gateway into the American grid, caught national attention and concern.

"The attack on Suffolk County occurred not in some technological backwater but in one of the nation's most densely populated, tech-savvy regions."

The attack on Suffolk County occurred not in some technological backwater but in one of the nation's most densely populated, tech-savvy regions. While Suffolk is best known as the home of the Hampton's – the glitzy haven for moguls from entertainment and high finance circles – it is also the location of the Department of Energy Brookhaven National Lab, one of the federal government's largest high-tech research facilities, which has spawned seven Nobel prize-winning discoveries. Also within Suffolk County resides the Cold Spring Harbor Lab, a federally-backed private research facility where the double helix structure of DNA was first identified, and which employs more than 600 scientists, many working on the most promising cancer research.

October 4, 2022

October 9 2022

October 14, 2022

"It is critical all levels of government take the threat from China seriously," said Brian Murphy, former acting Under Secretary at the U.S. Department of Homeland Security, and CIO, CISO and Chief Counterintelligence Officer. "There is a belief in some American towns and cities that 'it won't happen here.' But such a view is mistaken. A nation-state such as China steals data for a range of reasons. It could be to acquire intellectual property, or to plant malware for future endeavors. They also harvest data to prepare cognitive influence operations. They aggressively target state and local entities."

The status of the investigation into the Suffolk attack is not clear. Media has reported that the Suffolk County District Attorney – a recently elected official whose predecessor mishandled an earlier investigation – is working with the FBI to investigate the causes and long-term impact of the breach. The County legislature has hired a former federal prosecutor to conduct an independent investigation, but no substantive report has been issued.

Government entities must bolster their cyber defenses

The Chinese government has a long history of collaborating with independent hackers to expand its reach while providing a veneer of deniability. Information stolen from Suffolk County is likely to have more long-term value; allowing Chinese intelligence to develop personal profiles of American citizens that includes spending and lifestyle habits. Over the years, Beijing's operation has evolved from the simplicity of inept thugs utilizing patently phony emails and similar techniques to break into American public and private systems to the emergence of savvy operators. "They operate more like a professional intelligence service than the smash-and-grab operators we saw in the past," the head of a leading cyber security firm told the New York Times last year.

"Over the years, Beijing's operation has evolved from the simplicity of inept thugs utilizing patently phony emails and similar techniques to break into American public and private systems to the emergence of savvy operators."

The FBI has recently warned that the Chinese government is using stolen personal identification information to target Chinese nationals residing here, including U.S. citizens, as part of a "campaign to export repression."

Beyond targeting individuals, Chinese intelligence agencies have been known to use the personal information of U.S. citizens to focus on business strategies that could prove valuable during periods of heightened conflict. Early in the Covid pandemic, Chinese labs offered services to American consumers that the U.S. government warned were a cover for collecting DNA and similar information. This information could be especially useful to the Chinese pharma industry that hopes to control and strangle the supply of necessary medicines.

October 16, 2022

October 27 2022

October 30, 2022

According to a report released in March by the Center for Strategic and International Studies, the shift from quick-hit economic hacks to the search for long-term strategic information has been going on for over a decade.

The Suffolk hack in detail

After the attack forced officials to shut down the county's network in September 2022, officials funded a full forensic examination by Palo Alto Networks. This California cybersecurity firm had conducted earlier work on the system.

"After the attack forced officials to shut down the county's network in September 2022, officials funded a full forensic examination by Palo Alto Networks."

The hackers made "initial access" on Dec. 19, 2021, "leveraging a Log4J vulnerability exploit" and "established persistence and a command-and-control connection," according to a three-page summary prepared for county legislators by Palo Alto Networks.

The lurking software vulnerability that exposed machines around the globe was initially spotted a week and a half earlier, on Dec. 9, 2021, by a private user, leading to an international notification from the open source, Apache Software Foundation. Two days later, the U.S. Cybersecurity and Infrastructure Security Agency ("CISA) issued a terrifying warning.

"This vulnerability, which is widely exploited by a growing set of threat actors, presents an urgent challenge to network defenders given its broad use.... To be clear, this vulnerability poses a severe risk." The warning from the CISA, the Department of Homeland Security's lead cyber safety agency, "compels federal civilian agencies -- and signals to non-federal partners -- to urgently patch or remediate this vulnerability."

Functional patches to override the vulnerability were available on Dec. 17, 2021, according to a follow-up alert from CISA. There is no indication that the warning resulted in any action within Suffolk County government, even as hackers securely planted their pirate flag in Riverhead on December 19. Chinese hackers immediately targeted the newly identified vulnerability.

A hacking group known as APT41 began slamming computer systems around the globe "within hours." The Wall Street Journal reported that the flaw could impact "hundreds of millions of devices" and that hackers were executing "millions of attempts" at intrusion within days.

Mandiant, a cybersecurity firm that Google Cloud has recently purchased, identified APT41 as a "Chinese state-sponsored espionage group" that started as a criminal rogue operation in 2012, shifting to government-driven espionage three years later. Within days of the Log4J discovery, the Chinese group hit targets in 14 countries, including financial, healthcare, media, and government agencies. CISA said the glitch allows the "adversary to take full control over the system," including the ability to "steal information, launch ransomware, or conduct other malicious activity."

November 3, 2022

November 14 2022

November 24 2022

Three months after the international warning, the mysterious hackers on Long Island "continued to bypass network security and install remote monitoring and management tools as they began harvesting clerk user credentials" inside Suffolk systems.

A month later, in April, hackers created a user codenamed "John" with full administrative access.

In June, another account was created that gave the hackers full access to the entire system from an unnamed remote location.

By July, the group had installed and unleashed Cobalt Strike, a notorious tool used by hackers for ransom, data theft, and intelligence purposes. By August, the group had leapfrogged into the larger and more sensitive county system.

The hidden attack was discovered by county workers. "On September 8, 2022, ransomware encrypted files and left ransom notes in the County, Clerk, and Health environments," the report said. The group requested a $2.6 million ransom to release files and retreat. On Sept. 11, County Executive Steve Bellone gave a press conference with the first description of the scale of the attack and declaring a state of emergency.

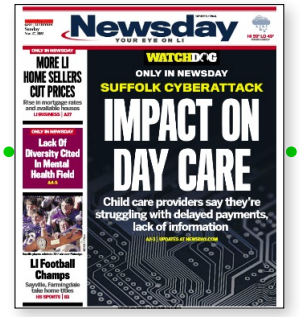
The still anonymous hackers issued a statement on the dark web: "Extracted files include Suffolk County Court records, sheriff's office records, contracts with the state of New York, and other personal data of Suffolk County citizens. We also have huge databases of Suffolk County citizens…" and posted several examples of purloined information, including speeding tickets and a handwritten marriage license from 1908.

"The 911 emergency response system was slammed as things like geo-location capabilities froze, sending operators scrambling to paper maps to direct police and ambulances."

The county refused to pay the ransom and shut down all systems.

Over the coming weeks, chaos reigned as the local government was driven back to the days of pen and ink, fax machines, and other archaic technology. This slowdown delayed millions of dollars' worth of guaranteed payments to contractors and local entities, crippling the local real estate market that relied on computer files to conduct title searches and cut off county emails. Local officials published addresses from private accounts like Gmail to maintain constituent contact.

The 911 emergency response system was slammed as things like geo-location capabilities froze, sending operators scrambling to paper maps to direct police and ambulances. Police temporarily lost the ability to run warrant checks from patrol cars and the system was so overwhelmed, the local New York Police Department (NYPD) and New York State Police sent officers to assist. It is unclear if any fugitives escaped apprehension or if medical issues were complicated by the lagged response. Most computer services returned by February.



November 27, 2022

November 30, 2022

December 2, 2022

The aftermath and the blame game

On April 12, Bellone released to the County Legislature a heavily redacted report from Palo Alto Networks detailing the number of incursions, and it did not identify the groups responsible. As of this writing, several services still remain down, including online property searches and sewer bill payments.

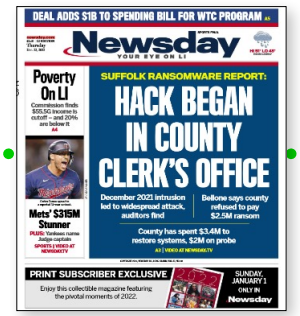
Possible Chinese involvement goes unmentioned, with Suffolk officials publicly focused on internal political rivalries. When Bellone released the redacted Palo Alto Networks report, he held a 20-minute press conference lambasting the former County Clerk. He had earlier said that part of the blame for the attack should be laid at the feet of IT supervisor Christopher Naples who was running a surreptitious Bitcoin operation in the clerk's technology center. Bellone alleged that Naples blocked the installation of protective software to protect his mining operation. While those details remain unclear, what is clear is that the county failed to conduct a robust review of computer security for months after Naples' operation was uncovered.

Court records indicate an employee in the clerk's office first spotted one or more rogue machines hidden in the Clerk's Technology Center in Riverhead in February of 2019 but did not report the finding, fearing it might annoy his supervisor. A year later, another employee spotted unauthorized computers, took photographs, and forwarded them to a county supervisor who was not involved in daily operations in the clerk's center. Court papers suggest the discovery was forwarded to the DA's office, but it wasn't until July and the filing of a more specific notice that prosecutors overtly acted. On July 29, 2021, investigators from the DA's office made an after-hours visit to the clerk's center and identified 21 illegally installed Bitcoin computers. Three weeks later, they returned with a search warrant and seized 46 illegal computers, routers, and an antenna that could facilitate unauthorized external access. That day, Naples told law enforcement that he had installed the machines to mine Bitcoin for his own financial gain. Weeks later, he surrendered to authorities on Sept. 8, 2021, charged with three felonies. He was released without bail and remained on the county payroll.

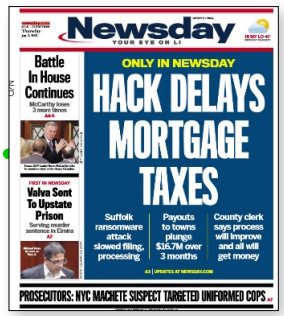
"Court records indicate an employee in the clerk's office first spotted one or more rogue machines hidden in the Clerk's Technology Center in Riverhead in February of 2019 but did not report the finding, fearing it might annoy his supervisor."

Then-DA Timothy Sini announced the arrest, focusing on Naples' theft of electricity to operate his Bitcoin minters, making no mention of other security issues. Naples' boss, County Clerk Judith Pascale, also downplayed any further impact. "The public can be assured that no Suffolk County records were accessed, misused, or impacted by the conduct being investigated by the District Attorney's Office," Pascale said, according to Newsday.

December 4, 2022



December 22, 2022



January 5, 2023

Whether Pascale, who was voted out of office later that year, was correct regarding the sanctity of data and the Bitcoin computers is not clear. County officials seem satisfied with the public perception that Naples' Bitcoin machines were responsible for the hack rather than publicly implicating foreign intelligence.

At a December 2022 press conference, County Executive Bellone alleged that Naples had delayed implementing requests for enhanced firewalls that would have prevented the attack, preferring to delay the discovery of his Bitcoin operation.

"County officials seem satisfied with the public perception that Naples' Bitcoin machines were responsible for the hack rather than publicly implicating foreign intelligence."

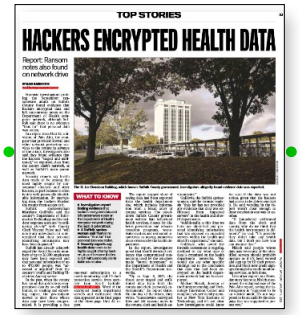
Outside experts are puzzled by Naples' status – free without having to post bail, having not faced a grand jury 20 months after being fingerprinted, and still receiving a bi-weekly county paycheck. "If the county's computer collapse was Naples' fault, he seems to be getting off easy," declares a former federal law enforcement official. "He fits the profile of a cooperating witness, but if that's the case, who the heck is he ratting out nearly two years later? It just doesn't make sense."

The lack of grand jury action has left the case and the scant collection of public files regarding his crimes in the Southampton Justice Court; a small facility hidden next to the town's waste transfer facility. Files from that courthouse are not available on the statewide computer system that provides public and media access to case files. Not only is the slapdash facility a three-hour drive from the nation's media capital, but access to the files is also tightly restricted. The court building has a standing ban on copying devices like cell phones and cameras – a ban enforced by armed officials and metal detectors. Clerks in the courthouse acknowledged that the Naples case is one of the oldest in the courthouse. Clerks closely monitor public access to files, peering over the shoulder of members of the public who exercise their right to inspect public files, scolding any attempt to even peruse the file folder cover of the Naples case without explaining why any notations might be confidential.

Naples is scheduled to return to the tiny courthouse next month. However, there has yet to be any clear indication or conclusion that his illegal activity had any connection to the hack.

The consequences of ongoing cybersecurity complacency

The history of computer security practices by the Suffolk County government is filled with egregious errors. The biggest mistakes stem from political finger pointing. Additionally, most of the county government's computer systems were siloed rather than controlled by a single unified entity.


TOP STORIES
HACKERS ENCRYPTED HEALTH DATA
Report: Ransom notes also found on network drive

January 8, 2023


Newsday
YOUR EYE ON LI
ONLY IN NEWSDAY
CYBER WAKE-UP CALL ON LI
Alarmed by Suffolk ransomware attack, town and village officials say they're reevaluating security
It's Almost Over
Blinken Cancels Trip To China Over Balloon
KYRIE IRVING SEEKS TRADE FROM NETS

February 4, 2023


Newsday
YOUR EYE ON LI
ONLY IN NEWSDAY
SUFFOLK CYBERATTACK
THE INSURANCE QUESTION
County says it was ineligible for a policy
Experts say lack of coverage may have signaled county's vulnerability before '22 intrusion
Call Centers: Can A.I. Solve Worker Shortage?
Mobile Clinic Teaches Students, Treats Public
Dick Cavett Is Talking — About His Life

March 5, 2023

In 2018, the county legislature passed resolution - 1132-2018 – mandating the County Executive carry out an annual cybersecurity risk assessment. Implementation was delayed, and a year later, a similar mandate came from the legislature, leading to the issuance of a report in January 2020.

The report was primarily created by an outside contractor, RedLand Strategies, a consulting firm run by former State Senator Michael Balboni, and Palo Alto Networks.

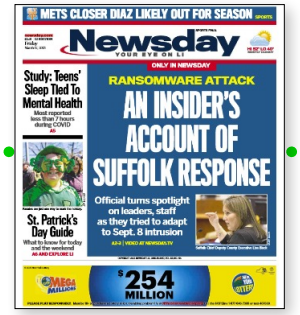
Balboni, a Republican from East Williston, left the State Senate in 2007 to become deputy secretary for Public Safety and Homeland Security Advisor for then-Governor Elliot Spitzer, a Democrat. Balboni developed some security credentials during his time in government, but is an attorney, not a cybersecurity expert. After leaving government, he created RedLand to cash in on that cachet. It is a three-person operation with another lawyer who worked as an advisor for New York state homeland security operations and Balboni's wife, Stephanie, who has a master's degree in special education. RedLand has substantial business with governments, including a $120,000 contract to assist the Nassau County Police in implementing police body-worn cameras.

"The history of computer security practices by the Suffolk County government is filled with egregious errors. The biggest mistakes stem from political finger pointing."

The report's first recommendation was to hire a Chief Information Security Officer (CISO) who would have authority not only over the county's main system, but also over the related systems in places like the clerk's offices, courts, and police departments. Most major corporations and government agencies employ a CISO because of their technical expertise. Officials in Hauppauge, a small hamlet in Suffolk County, blamed the delay in filling the position on the pandemic. At the time of the attack, county cybersecurity was overseen by Brian Bartholomew, the information technology security coordinator. He retired in 2021 but remained in charge, working as a consultant from his new home in Florida.

In February, Suffolk announced they were finally prepared to hire a CISO and had hired Balboni to lead the search. Balboni had recommended county contracts for Palo Alto Networks. Newsday later revealed that RedLand was working as a Palo Alto lobbyist, paid to help the company win government contracts. It is not clear if Steve Bellone was aware of the relationship, however he has continued to support both firms.

In June of 2022, while hackers were having their way with county computers, a warning came to the office of Raymond Tierney, who replaced Sini as District Attorney.



March 17, 2023

April 9, 2023

May 1, 2023

The tip from an unnamed FBI agent was passed through a court clerk and alleged that a cyber breach was "taking place." Tierney, who was not involved in Naples' arrest but whose office currently oversees the stagnant case, passed on the information to Bartholomew. He replied that he was unaware of any threat, adding that "none of my equipment is lighting up" as it should in case of an attack, according to Newsday. The story said Tierney was told the county had contacted the FBI.

The level of local naivete was further shown by a Newsday story in March reporting county government hadn't bothered to apply for computer insurance that would have covered damages and paid a requested ransom. The official excuse was that officials were aware their systems failed to meet minimum security requirements, leaving the county ineligible for coverage. Instead of addressing the shortcomings, government officials did next to nothing and left the county unprotected by specialized insurance that would cover a ransom and investigative costs.

"The sad truth is that the Suffolk County hack represents the alarming degree of complacency, inefficiency and ignorance surrounding the cybersecurity landscape within critical government and business entities."

"If you want to insure a building, the building has to be up to code," said Justin Cappos, an associate professor of computer science and engineering at the Tandon School of Engineering at New York University, in a statement to Newsday. He and others were astounded by Bellone's statement that the county was "ineligible," saying a few proactive fixes could have solved the insurance issue.

The sad truth is that the Suffolk County hack represents the alarming degree of complacency, inefficiency and ignorance surrounding the cybersecurity landscape within critical government and business entities. Without greater enforcement of established minimum regulatory requirements, penalties for compliance failures, and strong accountabililty policies this chaotic breach scenario will play out in counties across the nation.

Keep Your Enterprise Protected.
Get a Demo or Free Evaluation.

To learn more, visit www.revbits.com

RevBits®

34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • www.revbits.com