ARTIFICIAL INTELLIGENCE

AI is a double-edged sword in muni issuer cybersecurity

By Colin Royal

Published July 22, 2026, 10:04 a.m. EDT
Updated July 22, 2026, 10:09 a.m. EDT
4 Min Read

"We're in an interesting time where a lot of our normal processes and procedures are under attack with AI," Basefund CEO and co-founder Robert White said. "We're in a stage where we need to transition to

more robust security procedures."

The growth of artificial intelligence allows developers to find vulnerabilities within code faster, but cybercriminals can also discover new ways to bypass security.

"We're in an interesting time where a lot of our normal processes and procedures are under attack with AI," Basefund CEO and co-founder Robert White said. "We're in a stage where we need to transition to more robust security procedures."

Advanced technology is becoming more integrated into public finance. As issuers explore new opportunities and ways to push the market forward, they've encountered additional cyber-related risks.

States experimenting with cryptocurrency open themselves to cyberattacks, the risk of which increases as the amount of digital assets that they hold grows, according to a recent Moody's Ratings report.

"State and local governments that hold cryptocurrencies like Bitcoin, face significant cyber risks due to the fundamentally digital and decentralized nature of these assets," according to the report. "Storing cryptocurrency requires secure management of digital wallets and private keys, which, if compromised through hacking, phishing or insider threats, can lead to irreversible financial losses because of the immutable nature of the blockchain."

Cybercriminals and ransomware groups, see states with digital assets as appealing targets because of their "limited expertise compared with the private sector," according to the Moody's report.

"One of the most significant cyber-related threats facing municipal issuers today is business email compromise (BEC), where attackers gain access to or convincingly spoof trusted email accounts involved in a bond transaction," according to an Indiana Cybersecurity Hub blog post. "These attacks are designed to redirect wire transfers or alter payment instructions at critical stages, such as closing."

Many attackers target the fiscal officers of smaller issuers, especially those who are not likely to have the resources to maintain or employ cybersecurity professionals. Because the officers are "moving the money," they become the most immediate points of attack and they must have an extra level of caution, Indiana Bond Bank Executive Director Jacob Blasdel said.

"The idea that these attacks are theoretical and hypothetical is gone now," Blasdel said. "I think people see [cyberattacks] coming to their front door, and it's causing people to take it more seriously."

States that are slow to acknowledge the need for augmented cybersecurity are also at risk. Refusing to update older systems could leave issuers at the mercy of cybercriminals.

"Legacy systems and legacy code that people have relied upon for many years have been the gold standard. Familiarity with those systems is a good thing,"Basefund's White said. "But, when it comes to AI, no matter how good older code and coders are, it can instantly find ways to break in and cause havoc."

In an effort to mitigate risk, some issuers have devoted funding to cybersecurity efforts. For instance, New York City announced a financial plan that involves the city's Office of Cyber Command receiving "approximately $105.8 million for fiscal years 2026 and $104.3 million for fiscal year 2027 and 2028," according to an offering statement from the city's $2.3 billion GO deal in March.

Indiana, meanwhile, is exploring how to best train municipal issuers within the state to prepare themselves to defend against cyberattacks.

"When we're issuing bonds for a local municipality, we're requiring that they know how to deal with things, but, more importantly, that they have a response plan in place in case they have a cybersecurity incident," Indiana State Treasurer Daniel Elliott said.

Elliott recommended in a co-authored article that issuers continue cyber education for employees, develop stronger training programs, use encryption for sensitive financial information, validate all third parties involved in a transaction, plan ahead for potential incidents, report incidents immediately and implement transaction verification protocols.

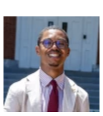
Cyber-education and training are only the beginning.

"I wouldn't say you stop doing education, but we have to start by expanding our security and our systems to be better for us instead of allowing people to try to be better against highly sophisticated systems," Basefund's White said.

"We need to recognize that we're going to have to look at all of these tools and make sure that issuers are using them," Elliott said. "Because if we don't, someone else is going to and that person may not have the best interest of the bond market in mind."

Both think that to be adequately protected, issuers must upgrade their cybersecurity systems. Eventual implementation of passkeys and biometrics will provide stronger and safer security, White said, but, for now, issuers should incorporate AI to enhance cybersecurity.

"The people that can build with AI, against AI, and for AI can honestly provide a more secure fence around it," he said.



Colin Royal

Colin Royal is a recent graduate of Morehouse College, and current NYU graduate journalism student.At Morehouse, he obtained the distinction of... Read full bio

ARTIFICIAL INTELLIGENCE CYBER SECURITY MUNIS PUBLIC FINANCE ATTORNEYS

RELATED

1 School districts face escalating cyber threat

2 Muni blockchain and tokenization: Evolution not revolution

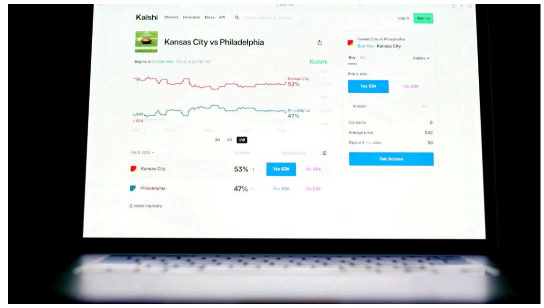
3 Data center financing assumptions under scrutiny

4 California's AI revenue windfall masks structural deficits

5 Federal funding cuts could drastically harm healthcare sector

MORE FROM THE BOND BUYER

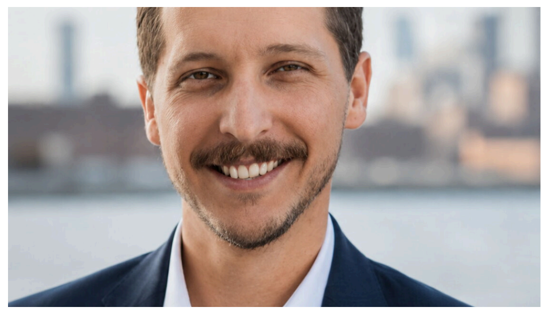
Prediction markets bring risks, opportunity for munis



Financial markets have embraced prediction markets as a mainstream crowdsourced provider of real-time probability signals and risk-hedging tools.

Jul 8, 2026

Cryptocurrency initiatives distract the muni market, observers say



Muni market professionals think state-specific crypto initiatives could distract from needed digital improvements to the market.

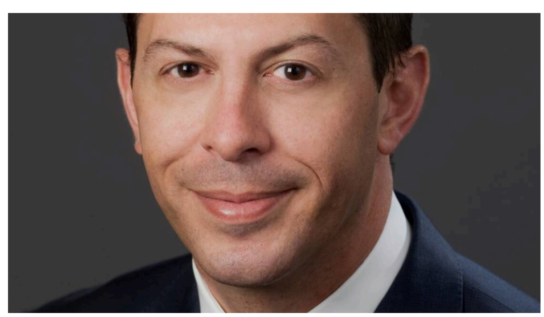
Jul 20, 2026

Investors to issuers: take our calls

SMAs are a "shoot now, ask questions later" type of buyer, said Dan Close, head of Nuveen's municipal fixed income team.

Jun 30, 2026

Redefining bond market leadership



The modern bond market is no longer defined by dealers and asset managers alone.

Jul 1, 2026

What's more important: AI optimization or employee training?

The optimization of fixed-income portfolios using AI may come at the cost of training the next generation of muni market analysts and portfolio managers.

Jul 9, 2026

Amid changing disaster landscape, Bernardi releases risk index

Illinois-based Bernardi Securities released an Environmental Risk Index that gauges relative environmental risk within municipal bond portfolios.

Jul 1, 2026