# US exchanges offer a rich potential target for hackers

May 26 2021, by Daniel Hoffman


Major exchanges say they are mitigating the risk of a cyberattack, but decline to elaborate on the specific steps they are taking.

Cyberattacks have long been seen as a threat to financial markets, but worries are becoming even more acute following a US pipeline hack that

set off a public panic and forced the company to pay a ransom.

Financial exchanges that manage daily transactions of tens or hundreds of billions of dollars are an appealing target for hackers.

Major stock exchanges insist they are on top of the issue, but remain mum about what steps they are taking to safeguard their networks.

"Technology and operational resiliency sits at the heart of everything we do," a Nasdaq spokesperson told AFP.

Likewise, the Chicago Board Options Exchange "takes cybersecurity very seriously and does not discuss our cyber defenses publicly," an exchange spokesperson said.

New York Stock Exchange President Stacey Cunningham told CNBC the exchange is "constantly working not only with our own teams but with others in the market, with the regulators and other exchanges on ensuring that markets are secure."

The Chicago Mercantile Exchange, a key trading venue for energy and agricultural products, declined comment entirely.

Recent history shows the hacking risk is far from a theoretical problem at financial exchanges.

Last August, New Zealand's NZX was crippled for four days following a digital siege.

The episode, a "distributed denial-of-service" attack, is a common type of cyberincident in which hackers saturate a system by sending a huge flood of requests, overwhelming the system and slowing or freezing operations.

"NZX has been advised by independent cyber specialists that the attacks ... are among the largest, most well-resourced and sophisticated they have ever seen in New Zealand," said NZX Chief Executive Mark Peterson said following the incident.

Such a calamity has yet to befall an exchange or major financial firm in the United States. But the worry has preoccupied US finance and government at the highest levels.

Federal Reserve Chair Jerome Powell told the news show "60 Minutes" last month that a cyberattack poses risks to financial markets even more severe than the liquidity freeze-up in the 2008 financial crisis.

"There are scenarios in which a large payment utility, for example, breaks down and the payment system can't work," Powell said. "Payments can't be completed.

"There are scenarios in which a large financial institution would lose the ability to track the payments that it's making."

Nasdaq employs resources to counter cyberthreats, but warns that "these measures may prove insufficient depending upon the attack or threat posed," the company said in a securities filing, adding that it "may be required to devote significant additional resources to the effort."

## Range of motivations

The most typical means used by hackers to extort victims is to infiltrate a computer network with ransomware, which encrypts the system's data that can be lifted after the ransom is paid.

Earlier this month, Colonial Pipeline, which provides gasoline to much of the US East coast, ultimately paid some $4.4 million to hackers after

the network was completely taken down for several days, sparking panic buying and a fuel shortage in some areas.

But money is not the only motivation for groups that might seek to take hostage a high-profile institution like a stock market, experts say.

"They may want to make money, damage the ability of the target to conduct business, steal sensitive information, or ruin their reputation," said Sean Cordero, a security advisor at Netenrich, a California cybersecurity company.

"Or, it could be all of the above and more."

The group's motivation also will determine the nature of the attack.

"If they are driven by espionage or are purely interested in gathering information, they would likely lay quiet and move discretely so that they may maintain access for as long as possible," said Alec Alvarado, a cyberintelligence specialist at Digital Shadows, a San Francisco company.

But groups seeking a large ransom payment may opt to inflict maximum immediate harm to elicit a quick response.

The range of motivations means firms should aim to make themselves "the hardest target" possible to thwart attacks, Alvarado said.

"Unfortunately, with ever-expanding attack surfaces, if a threat actor is willing to take the time to find a way in, chances are they probably will."

Cordero said frequent updates of security systems are needed to counter cyberrisks, requiring systems to be temporarily taken offline.

"This is ultimately a risk-based decision that can have major implications if not treated as such," Cordero said. "Unfortunately, these decisions tend to be relegated to the 'to-do' list and may go for months or years without action."