NYSE Insists It Was Not Victim of a Hack, but Questions Remain

BY LEAH MCGRATH GOODMAN 7/11/15 AT 10:55 AM

A plaque outside the New York Stock Exchange’s $600 million Mahwah, New Jersey data center, surrounded by sycamore trees, touts the 400,000-square-foot facility as “the most technologically advanced financial marketplace in the world.”

It’s also the back-up site of the world’s largest stock exchange by both market capitalization and trading value, with listed companies valued at nearly $20 trillion—the oldest exchange as well, considered “critical” to the nation’s financial infrastructure by the U.S. Department of Homeland Security (DHS).

Yet the 5-year-old facility struggled this week to take on the burden of the exchange’s trades, valued at more than $150 billion a day, even as volumes choked off during a nearly four-hour-long shutdown that began Wednesday at 11.32 a.m. ET and ended just 50 minutes before the market closed for the day, at 3.10 p.m.

Try Newsweek for only $1.25 per week

The NYSE has since said there were problems with its systems resulting from an overnight “software release,” saying the issue began well before the market opened and grew worse until the exchange halted trading. But many questions remain unanswered. While the market has largely recovered, the NYSE confirmed to Newsweek it is launching an internal investigation into the circumstances surrounding the outage and how to prevent recurrences. The NYSE’s regulator, the Securities and Exchange Commission, also will be conducting a review of its findings.

Thus far, the NYSE has definitively ruled out a cyber attack on the exchange, but a high-ranking official at the SEC told Newsweek on Friday the nation’s stock market regulator is not ready to rule out a cyber breach.
On Thursday, SEC Chairman Mary Jo White, who spoke by telephone to NYSE Chairman Jeff Sprecher during Wednesday’s outage, instructed the SEC’s director of trading and markets, Steve Luparello, to meet with senior NYSE officials Thursday. The meeting included NYSE President Tom Farley, a second official at the SEC told Newsweek. Both the NYSE and the SEC declined to discuss specific details of the meeting.

Late Thursday, a statement was issued by the SEC noting that the meeting addressed outage “events and NYSE’s plans going forward,” but did not elaborate. “The [SEC] chair and senior commission staff are continuing their discussions with exchange officials and other market participants,” it said. The SEC declined to comment Friday on whether the talks touched on the performance of the NYSE’s back-up facility, which took more than three and a half hours to kick in.

Pivoting to a back-up facility is not as easy as just throwing a switch, says Larry Tabb, founder and chief executive of market consultancy Tabb Group in New York. “They would need to move the orders, positions, data, configuration,” he says. “They would also need to move all of their client connections—this is huge, there would be thousands of connections that would need to be shifted and then shifted back. That is probably the real reason” for the delay, he added.

Other top brass in the U.S. government are monitoring the situation. President Barack Obama was briefed by Homeland Security Advisor Lisa Monaco earlier in the week. White House spokesman Josh Earnest backed the NYSE’s contention that no cyber breach had taken place, but did acknowledge reports of concurrent technology glitches Wednesday, as United Airlines suffered a “router issue” that grounded or delayed at least 800 flights, and The Wall Street Journal's website ran into “technical difficulties,” sending traffic to another site.

“There is no indication at this point either that there is malicious activity involved or that it was related to any of the other high-profile technology issues that have cropped up today,” Earnest said.

U.S. Treasury Secretary Jack Lew, who chairs the nation’s Financial Stability Oversight Council, created in the wake of the 2008–2009 credit crisis, is also being updated, according to a second White House spokesman.
In an initial autopsy of the outage released Thursday by the NYSE, the exchange said a software release conducted Tuesday night on a single trading unit (this is an engine that matches the trades of buyers and sellers of stocks) resulted in “communication issues” between customers requesting trades and the exchange’s trade-matching engine. The communication issues began at 7 a.m., the exchange said, well before the market opened at 9:30 a.m.

After the open, the exchange said there were “additional communication issues,” affecting other trading units and forcing the NYSE to shut the market down by late morning. The NYSE has not yet described the issues in more detail and declined to elaborate further Friday.

So far, the exchange has not explained how communication problems between customers and the single trading unit somehow cascaded into issues affecting all the NYSE’s customer gateways, which convey the communications, as well as other trading units. It is the exchange’s practice to deploy software for one unit at a time to avoid such an outcome. It confirmed in its statement it did so in this case. How the wider contagion spread to multiple units, forcing the shutdown, remains unclear.

A spokeswoman for NYSE wasn’t immediately able to comment Friday because of the ongoing investigation. She also declined comment on how the exchange was able to rule out a data breach.

While the complexity of trading technology has led to a higher frequency of trading glitches, software snafus and many a blunder in recent years on Wall Street, so too are market regulators, traders and politicians increasingly on notice for possible terrorist or cyber attacks.

As soon as the NYSE began to experience problems Wednesday, the U.S. Federal Bureau of Investigation was put on notice, says FBI spokeswoman Adrienne Senatore, who is in touch with the agency’s cyber squad at the New York field office. “Initially, we thought we might be the point of contact, but as the afternoon went on, it seemed clear that we wouldn’t be,” she says. At present, there is no FBI investigation into the outage under way, she says, but adds that the office is still “aware and monitoring the situation.”

FBI Director James Comey also weighed in. “In my business, you don’t love coincidences,” he told Congress earlier this week. “But it does appear there is not a cyber-intrusion involved.”
With government statistics showing American corporations are coming under cyber attacks for an average of 279 days before becoming aware of them, the FBI has put apprehending cybercrime at the top of its priority list in 2015.

Concerns about a cyber attack played out this week on Twitter, starting with a warning released Tuesday night, hours before the NYSE outage, from an account that appeared to be linked with the international hacker and activist group Anonymous, stating, “Wonder if tomorrow is going to be bad for Wall Street... we can only hope.”

In the aftermath of the outage, the NYSE ruled out a cyber attack, tweeting from its own account, “The issue we are experiencing is an internal technical issue and is not the result of a cyber breach.”

If there had been a cyber attack, the White House spokesman said, the National Cybersecurity and Communications Integration Center—a division of the Department of Homeland Security—should have been contacted by the NYSE or at least alerted to the potential of an attack, “and it wasn’t,” he says. The 24-hour, seven-days-a-week DHS outpost is responsible for protecting critical infrastructure like the NYSE from physical and cyber threats as part of a public-private partnership endorsed in January by President Obama.

The Department of Homeland Security, which has no regulatory authority over the NYSE and would have to be invited by the exchange to investigate any outage, said it hasn’t been, but is aware of the message from Anonymous. A DHS spokesman told Newsweek that, since the message from Anonymous did not specifically refer to the stock market or NYSE, nor claim explicit responsibility for the outage itself, there is little reason to investigate at this time. The SEC, NYSE and White House told Newsweek they were made aware of the message by the end of this week but had no comment on it.

In fact, no agency or regulator has directly investigated the NYSE outage or the Anonymous message, according to all the agencies Newsweek interviewed. According to the second White House spokesman, updates from the NYSE have been sufficient, noting that “they are a valued and trusted partner.”

Taking this on faith was not as easy for everybody.
“Given the NYSE’s terse statements, it is impossible to rule out the possibility of a cyber breach,” says Campbell Harvey, professor at Duke University’s business school. “The NYSE is a prime target. A marquee property. And my guess is that they’re under attack all the time.”

Rather than ruling out a hack on the exchange before an investigation is concluded, he suggests, “Why wouldn’t we want to deploy the nation’s resources to find out? Given that Homeland and the FBI are available, what is the downside? That’s what our tax dollars pay for.”