As cyber attacks detonate, banks gird for battle

July 16 2013, by Christina Rexrode

In this photo the website of the United State's biggest bank, JPMorgan Chase, is displayed on a computer screen, Tuesday, July 16, 2013, in Atlanta. Banks large and small are girding for an elaborate drill this week that will test how they'd fare if hackers unleashed a powerful and coordinated attack against them. The exercise is being called "Quantum Dawn 2," and if the name sounds like a video game, it's also meant to convey the seriousness of a big threat. (AP Photo/David Goldman)

It's a war game, Wall Street style.

Banks large and small are girding for an elaborate drill this week that will test how they would fare if hackers unleashed a powerful and coordinated attack against them.

The exercise is being called "Quantum Dawn 2," and if the name sounds like a video game, it's also meant to convey the seriousness of the threat.

Cyberattacks on the banking industry are growing more frequent and sophisticated and the list of assailants is ever-changing: crime bosses who want money, "hacktivists" who want to make political statements, foreign governments that want to spy on U.S. companies. A successful, widespread attack on the industry would shake confidence in the banking system, and the possibility has banks and regulators on edge.

Jamie Dimon, CEO of the country's biggest bank, JPMorgan Chase, acknowledged that attacks are becoming more complex and dangerous, no longer carried out by "fairly simplistic" hackers commandeering people's personal computers.

"Now you're talking about state-sanctioned folks, hundreds of programmers," he said in a call with reporters this spring, "taking over not just PCs but servers and mainframes."

JPMorgan and its peers like Bank of America, Citigroup and Wells Fargo have signed up for Thursday's drill, which is being organized by Wall Street's biggest trade group, the Securities Industry and Financial Markets Association, or SIFMA.

About 50 banks and organizations will participate, including government agencies like the Treasury, the Department of Homeland Security, the Securities and Exchange Commission and the FBI.

A surveillance sign is posted outside a Bank of America branch on Peachtree Street, Tuesday, July 16, 2013, in Atlanta. Banks large and small are girding for an elaborate drill this week that will test how they'd fare if hackers unleashed a powerful and coordinated attack against them. The exercise is being called "Quantum Dawn 2," and if the name sounds like a video game, it's also meant to convey the seriousness of a big threat. (AP Photo/David Goldman)

During the drill, bank employees will be stationed at their normal offices, and will be blasted throughout the day with bits of information that could indicate an encroaching hacker attack. They'll monitor a simulated stock exchange for irregular trading and will be pressed to figure out what's going on and how to react while sharing information with regulators and each other.

As the name suggests, this isn't the first Quantum Dawn. The original drill was in November 2011, and it attracted scant attention and only

about half as many participants. But that was before a wave of cyberattacks last fall, when big banks were forced to temporarily shut down their websites after attackers bombarded them with traffic—akin to overwhelming a phone line with too many calls.

"If you went to banks three years ago, and said, 'What are your top five risks?', probably none of them would put cyber on there," said Karl Schimmeck, SIFMA's vice president for financial services operations. Now, he said, the calculation has changed.

THE BARRAGE: Software giant Symantec calculates that cyberattacks against U.S. businesses jumped 42 percent last year. Banks, though, are reluctant to give more details about how they're affected, financially or otherwise, for fear of becoming a target, and attacks often go undetected and unreported.

HIGH ALERT: Whatever the number, banks and the government are on high alert. President Barack Obama warned about international hacking against the banking industry in February's State of the Union address. He later met with JPMorgan CEO Dimon, Bank of America CEO Brian Moynihan and other business leaders to discuss the threat.

Big banks have started listing cyberattacks as a potential risk factor in filings for regulators and investors. The Office of the Comptroller of the Currency, which regulates national banks, recently held a call with community bankers to warn them that they're not free from danger either: Since September, attacks have been increasingly aimed at businesses with fewer than 250 employees, the OCC says.

IMPOSSIBLE VICTORY? Banks realize the threat isn't going away. If anything, the possibility of an online attack will grow as customers do more transactions online and banks outsource operations to other companies whose systems might not be as secure.

An ATM is displayed at a Wells Fargo bank, Tuesday, July 16, 2013, in Atlanta. Banks large and small are girding for an elaborate drill this week that will test how they'd fare if hackers unleashed a powerful and coordinated attack against them. The exercise is being called "Quantum Dawn 2," and if the name sounds like a video game, it's also meant to convey the seriousness of a big threat. (AP Photo/David Goldman)

Says Greg Garcia, a former DHS official who now runs the consulting firm Garcia Cyber Partners: "If someone asks, 'When are you going to stop cybercrime?' Well, when are you going to stop crime?"

YOUR MONEY: The banks downplay the risk of hackers tapping into any individual customer's account. For most, that will never happen, the banks say, and even if it did, the customer wouldn't be responsible. Customers would have to go through certain steps to get their money back, like filing a claim, showing that they weren't negligently tossing

their account information around and giving the bank time to investigate. But federal regulations protect retail customers from being held accountable when money is removed from their accounts without permission.

A DRILL BY ANY OTHER NAME: As for the title of Thursday's drill, the one that sounds more appropriate for an action movie than a bank security exercise, it came about during the creation of the original drill in 2011, which was organized by the Financial Services Sector Coordinating Council.

National security staff at the White House wanted exercises to have names, preferably with two words. According to the FSSCC, a federal government official who was involved in the planning suggested the title after noticing some media reports about the dawn of quantum computing.

Schimmeck points out that a similar exercise in Britain had a title at least as curious: It was called "Waking Shark."