BusinessMirror
A broader look at today's business

Next big bailout for U.S. banks could be forced by cyberattack

By Carter Dougherty
August 30, 2014

Bankers and U.S. officials have warned that cyber-terrorists will try to wreck the financial system's computer networks. What they aren't saying publicly is that taxpayers will probably have to cover much of the damage.

Even if customers don't lose money from a hacking assault on JPMorgan Chase & Co., the episode is a reminder that banks with the most sophisticated defenses are vulnerable. Treasury Department officials have quietly told bank insurers that in the event of a cataclysmic attack, they would activate a government backstop that doesn't explicitly cover electronic intrusions, two people briefed on the talks said.

"I can't foresee a situation where the president wouldn't do something via executive order," said Edward DeMarco, general counsel of the Risk Management Association, a professional group of the banking industry. "All we're talking about is the difference between the destruction of tangible property and intangible property."

The attack on New York-based JPMorgan, though limited in scope, underscored how cyber assaults are evolving in ferocity and sophistication, and turning more political, possibly as a prelude to the sort of event DeMarco describes.

Not simply an effort to steal money, the attack looted the bank of gigabytes of data from deep within JPMorgan's network. And bank security officials believe the hackers may have been aided by the Russian government, possibly as retribution for U.S. sanctions over the Ukraine war.

Worst-Case Event

A worst-case event that destroyed records, drained accounts and froze networks could hurt the economy on the scale of the terrorist attacks of Sept. 11, 2001. The government response, though, might be more akin to that following the 2008 credit meltdown, when the Federal Reserve invoked "unusual and exigent circumstances" to lend billions of dollars.

The government might have little choice but to step in after an attack large enough to threaten the financial system. Federal deposit insurance would apply only if a bank

failed, not if hackers drained accounts. The banks would have to tap their reserves and then their private insurance, which wouldn't be enough to cover all claims from a catastrophic event, DeMarco and other industry officials said.

Janet Napolitano, the Secretary of Homeland Security until August 2013, warned in her valedictory speech that the country will someday suffer a cyber Sept. 11 "that will have a serious effect on our lives, our economy, and the everyday functioning of our society."

Wall Street banks, brokerages and other companies have grown increasingly concerned as well. It's just a matter of time before nation-states or terrorist groups aim to "destroy data and machines," the industry's biggest lobbying group wrote in a June 27 internal document.

Economic Losses

The Insurance Information Institute, an industry group, estimates that policies paid out about $42.9 billion after the Sept. 11 attacks. Economic losses, given the closure of lower Manhattan, grounded flights and shuttered financial markets, were much larger.

Regulators are raising pressure on banks, broker-dealers and hedge funds to report intrusions and show they're improving cyber defenses. The June document, from the Securities Industry and Financial Markets Association, asked for federal help in those tasks, too. It proposed a government-industry cyber-war council to share threat information, help build firewalls and prevent attacks from spreading.

JPMorgan Investigation

Hackers burrowed into JPMorgan and siphoned off gigabytes of information, including customer-account data, according to two people familiar with the lender's investigation, who asked not to be identified. JPMorgan is taking additional steps to safeguard data and is working with government authorities to determine the scope of the assault, said Patricia Wexler, a spokeswoman for the bank.

Customers subject to unauthorized checking and savings account withdrawals that are promptly reported to JPMorgan will be reimbursed, according to a person with knowledge of the bank's policies. The bank hasn't seen unusual levels of fraud as of Friday afternoon, said the person, who asked not to be identified because the matter is private.

Discussions about the government's role in cleaning up after a catastrophic cyber assault have centered on the Terrorism Risk Insurance Act, or TRIA. States are also pressing Washington to clarify how the Stafford Act, the main statute for relief from natural disasters, would factor in.

Financial Support

The insurance law, enacted after the 2001 attacks, authorizes the government to provide financial support for insurance companies in the wake of terrorism. It is up for renewal this year. Under TRIA, insurers cover a fixed amount of losses from terrorist attacks with the government backstopping additional costs up to $100 billion. The law gives the Treasury secretary broad latitude to invoke the backstop.

In private meetings, Treasury officials have told insurance industry lobbyists that the department would treat cyber-terror like a physical attack under TRIA, said the people involved with the talks, who spoke on condition of anonymity because the discussions were private. Suzanne Elio, a Treasury spokeswoman, declined to comment on any private assurances.

As recently as last year, insurers were pressing Congress to add language about cyber attacks to the reauthorization bill. The industry has dropped that request for political reasons, said Mark Calabria, director of financial regulation studies at the Cato Institute and a former congressional staff member.

Senate Approval

While the Senate approved a renewal July 17, the House version sits with the Financial Services Committee. Representative Jeb Hensarling, a Texas Republican who is chairman of the panel, said he wants to narrow the program and eventually unwind it. Trying to expand its scope would draw Hensarling's ire, Calabria said.

"The industry doesn't want to open that fight up," Calabria said. "It would jeopardize renewal altogether."

Besides invoking the terror insurance law, federal officials might also find themselves under pressure to tap funds originally intended for natural disasters. The Federal Emergency Management Agency suggested in a 2012 report that physical damage resulting from a cyber attack could be covered by the existing law governing its work, the Stafford Act.

"In these big disasters, everyone is looking at the Stafford Act because there is money there," said Monica Giovachino, a managing director at CNA Corp., the Arlington, Virginia research firm that worked on the 2012 simulation.

Rendered Inoperative

Dan Watson, a spokesman for FEMA, said that the Stafford Act is "intended to be flexible." It comes into play when lives are on the line, or when important systems are "rendered inoperative," Watson said. "There's nothing particularly unique that would apply for a cyber-attack than any other disaster," he said.

Federal and state officials are planning a joint meeting in October to flesh out a recovery plan after a cyber-terror attack, the National Emergency Management Association, a group representing states, said on its website.

Insurance policies covering banks against hacking have been around since the 1990s, but only recently have they covered more serious damage, said Tracie Grella, global head of professional liability for American International Group Inc. Insurers have warned Treasury that they won't sell cyber policies if the government program isn't renewed.

"The limited market for cyber terrorism that does exist is reliant on TRIA's continuation beyond 2014," London-based insurer Aon Plc wrote in a paper sent to the Treasury last September.

New Policies

AIG in May began offering a new line of insurance in addition to previous policies for the costs of data breaches, hack investigations and business interruption. The new policies cover physical damages to people and property, such as inoperative computers or broken electrical grids.

Premiums paid to AIG on cyber policies rose about 25 percent a year in 2012 and 2013; so far this year they've risen by 30 percent, led by strong demand from financial firms, Grella said. The company doesn't disclose the amount of premiums paid.

"Especially the larger financial institutions have been looking at cyber insurance and buying it for some time," Grella said. "Pressure from the regulators will increase awareness among smaller firms." Other insurers offering cyber-attack coverage include Travelers Cos., Chubb Corp. and Ace Ltd.

Still, even expanding product lines can't solve the problem of a systemic crisis of the sort that Napolitano warned of, said Emily Freeman, a specialist in cyber-liability at Lockton Cos., a Kansas City-based insurer.

'Customer Trust'

"There are large areas of risks where there are no insurance solutions," Freeman said. "And one of those is when you have a crisis in customer trust."

The industry's most costly cyber events have been thefts, such as a $40 million debit-card break-in at an unnamed financial institution that U.S. regulators reported in April. In some cases, banks and depositors have been fighting in court over whose security breach was responsible for the hack.

The next wave of attacks probably will be more destructive and could result in "account balances and books and records being converted to zeros," according to the June

document from Sifma. Lawrence Mirel, a former insurance commissioner for the District of Columbia, said that without precedent it's difficult for insurers to estimate the possible damage.

"Nobody has really been able to define what cyber-terrorism risk is," said Mirel, now a partner at Nelson Levine de Luca & Hamilton LLC. "So even the companies that are offering these policies don't entirely know what they are covering."