Cybersecurity

Mexico Foiled a $110 Million Bank Heist, Then Kept It a Secret

By Michelle F Davis
May 29, 2018, 7:00 AM EDT

- Now, its banking system is being hit by a new wave of attacks
- Policy makers are being criticized for a lack of communication

A Banorte bank branch in Mexico City. *Photographer: Jonathan Levinson/Bloomberg*

On a Tuesday morning in early January, the computer system at Mexico's state-owned trade bank went haywire. Some of Bancomext's workers couldn't get their PCs to turn on. The internet was slow. Routine operations were taking longer than normal.

Inside the lender's concrete-and-glass building on the southern outskirts of Mexico City, a mid-level technician was monitoring messages coming in on the Swift network, the air-traffic control system for sending money around the world. His job was to check fund transfers to make sure they matched the payment orders dispatched by Swift.

That day, transaction volume was several times higher than normal. The worker scanned the messages from Swift until he discovered something: unusual activity at the Standard Chartered Plc account Bancomext used for international wires.

Bancomext would later learn that hackers suspected to be from North Korea had tried to siphon off more than $110 million, forcing the lender to temporarily suspend operations in its international payment platform. These accounts of cyberattacks are based on conversations with individuals briefed on the details of the incidents, who asked not to be identified because investigations by authorities haven't been completed.

Bangladesh Heist

Worldwide, a string of attacks targeting banks' connections to the Swift network has prompted financial institutions to enact new security measures, with the most famous invasion coming in 2016 when criminals attempted to steal $1 billion from the central bank of Bangladesh. But in Mexico, details surrounding the Bancomext assault have been kept secret by government authorities and the bank, meaning the nation's sprawling financial system never got the wake-up call that could have helped guard against a new series of intrusions that authorities are still trying to contain.

Just a few months after the Bancomext attack, hackers began hijacking Mexican financial institutions' connections to the country's domestic payment transfer system, known as SPEI. So far, they've gotten away with at least $15 million. While authorities don't know where the attacks originated, they suspect they were orchestrated by sophisticated parties who colluded with account holders to withdraw massive amounts of cash from bank branches around Mexico. Officials say they still aren't certain the thefts have ended.

"There's still a culture of reactivity when it comes to cyber risks," said Michael Rohrs, an associate director for Control Risks's information security practice in Washington. "All the news around the attempt against Bancomext and the Swift incident with the central bank of Bangladesh could have been a loud-enough wake-up call for the sector."

A representative for Bancomext said the lender followed all security protocols and communicated with authorities from the start. Press officials for Standard Chartered and Swift declined to comment.

SPEI-GATE*
How the attacks on Mexico's domestic payment system went down

Date	Event
April 17	Banxico detects first cyberattack
April 24	Two more financial firms hit
April 26	Fourth cyberattack
April 27	Banxico tells public it's detected "incidents"
April 30	Banxico asks a dozen banks to switch to backup SPEI
May 8	Fifth institution gets attacked
May 11	Banxico says Mexico AG probing incidents
May 14	Banxico says "incidents" were cyberattacks
May 15	New cybersecurity unit created within Banxico
May 16	Banxico says raids have resulted in $15m of thefts
May 17	Banxico places new limits on money withdrawals
May 18	Banxico head of payment systems leaves

Source: Bloomberg
* SPEI is Mexico's domestic payment transfer system, which is operated by the central bank, known as Banxico
Bloomberg

Cybersecurity professionals and bank executives who spoke to Bloomberg said the poor coordination among financial institutions and regulators helped propagate the recent raids targeting three lenders, a brokerage and a credit union. Knowing more about how the Bancomext assault and other cyber heists went down could have helped the firms protect themselves.

A central bank spokeswoman said that information sharing is very important, but that institutions coming under cyberattacks don't always report them because of concerns about their reputation. It's a matter of great to concern to the bank, she said. Case in point: the authority didn't learn about one of the breaches until about a week after it happened because the firm didn't immediately disclose it.

Workers Go Home

Officials say they don't have any reason to believe the current issues with domestic payment transfers are related to the attempted heist of Bancomext funds in January. While both were "man in the middle attacks," the central bank spokeswoman said, one targeted vulnerabilities in international payment systems, while the current spate of attacks affected Mexico's domestic wire system. The central bank has maintained an open line of communication with all SPEI participants since the first incident, the spokeswoman said.

Back at Bancomext's headquarters shortly after the Swift abnormalities were first discovered, executives took action. The lender, which has $13 billion of loans outstanding and is charged with promoting international trade, suspended operations and sent some workers home. Desk phones were turned off and the bank shut down its email server.

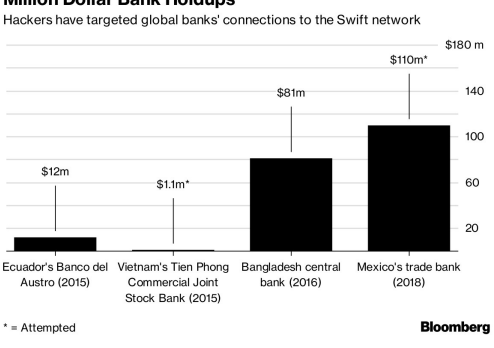
Officials soon discovered the unusual transactions were payments that had been disguised as a donation from the Mexican bank to a Korean church.

Luckily for Bancomext, it was after 3 a.m. in Seoul and since banks weren't yet open for the day, the money hadn't gone through. That bought the lender some time to get in contact with officials at Standard Chartered, who were able to stop the transfer.

Next Generation

Once the central bank was aware of Bancomext's issues, it directed some other banks to double-check the security of their operations, but it didn't provide them any detail about what to look for, according to two people with knowledge of the matter who asked not to be identified because the information is private. A spokeswoman said the level of detail the central bank provided reflected the amount of information it had at the time. Experts consulted by Bancomext would later tell the bank that hackers had managed to penetrate its Swift connection thanks to a so-called "next generation" virus that had probably been activated after an employee clicked on a malicious email attachment. It had likely sat undetected in the bank's systems for several months or even years, allowing hackers to assemble data on typical operations so it'd be easier to disguise the theft.

Million Dollar Bank Holdups
Hackers have targeted global banks' connections to the Swift network



* = Attempted
Bloomberg

In the more recent hack involving Mexico's domestic payment system, the perpetrators have so far managed to steal about 300 million pesos ($15 million). Ultimately, the affected institutions will be the ones on the hook for that money, the central bank has said.

The central bank first detected irregularities in a small financial institution's connection to the SPEI network April 17 but it didn't disclose it until 10 days later because the incident seemed like an isolated event.

About a week after the initial attack, officials at Grupo Financiero Banorte noticed hundreds of irregular transactions being dispatched through SPEI, according to a person familiar with the matter. The biggest Mexican bank had been the victim of a cyberattack just like the one discovered by the central bank the previous week. Banorte spokeswoman Veronica Reynold said the lender has acted in direct coordination with the central bank.

It wasn't until April 27, after the Banorte attack, that the central bank published a press release saying some financial firms had experienced "incidents" when operating the SPEI and that those firms would be connecting to the payment network via an alternate method that was more laborious but also more secure. Even then, the authority didn't mention a cyberattack.

No Names

By then, the central bank had knowledge that three firms' connections to the SPEI network had been compromised. On May 2, a fourth institution disclosed to the central bank that it had also been hacked the previous week. A week later, the number of hacked firms grew to five. The central bank still hasn't disclosed the names of the affected parties.

Top executives from four lenders in Mexico complained to Bloomberg that the central bank's decision to stay silent about details of the attacks made it harder to shore up their systems. Banorte hasn't had issues since it switched to the backup SPEI connection. But the authority didn't ask other banks to enact contingency plans until the following days and weeks.

In Latin America, Mexico ranks as the country with the most cyberattacks after Brazil, according to a January 2017 paper from the Wilson Center on security in the country. The financial sector has been hit with extortion attempts and denial-of-service schemes as well as trading platform disruptions, according to a 2015 Control Risks report.

No Fines

In the Bangladesh job, the thieves were able to get away with $81 million by sending fake Swift messages that tricked the Federal Reserve Bank of New York into wiring money to accounts in the Philippines. Swift has said its system hasn't been breached; rather security issues have originated in banks' systems.

Alejandro Diaz de Leon *Photographer: Susana Gonzalez/Bloomberg*

Last year, the central bank set rules related to the SPEI system that require financial institutions to have in place certain emergency response protocols for when attackers strike, among other requirements. Banxico evaluated financial institutions' adherence in January and found some banks weren't fully compliant, Governor Alejandro Diaz de Leon said in an interview May 18. So far, the authority hasn't levied any fines.

While the central bank hasn't been particularly forthcoming about the attacks, neither have the banks that were targeted gone out of their way to share what happened with other lenders. Cybersecurity analysts speculate that could be because they're afraid they'll get punished for not having sufficient controls and they don't want to give competitors any information that would give them a leg up.

Inside Job

But experts agree that sharing information makes the whole system stronger.

"It's so important that these banks talk to each other, that they share the best practices," said David Schwartz, chief executive officer of the Florida International Bankers Association, a Miami-based trade association. "There's not enough of that" in Mexico, he said.

There are plenty of theories around how the most recent hacks went down. Some suspect help from current or former central bank employees. Diaz de Leon has denied this. Others say hackers had access to the passwords to authentication tokens for accounts, which would suggest insiders at the respective banks may have helped them infiltrate their systems.

Mexico is finally taking steps in the wake of the SPEI scandal to ensure authorities and banks have a better way of sharing information with each other to be able to coordinate responses the next time criminals strike, the central bank governor said. The monetary authority is also creating a new division to set policies to better guard banking information.

Ignorance

"The idea is to have an understanding among authorities and financial entities that whenever you get some type of shock or cybersecurity event, you should share it, and everyone will have information and clarity about what's going on," Diaz de Leon said.

Up until now, online security hasn't been taken seriously in Mexico's banking sector, according to Federico De Noriega, a partner in the finance group at Hogan Lovells in Mexico City. He cited his experience representing a foreign insurance company that was marketing policies to protect against cyberattacks to financial institutions in Mexico.

"There was a lot of ignorance," De Noriega said. "That tells you people aren't aware of this risk, or they're not taking it seriously. I think they'll start taking it more seriously now."