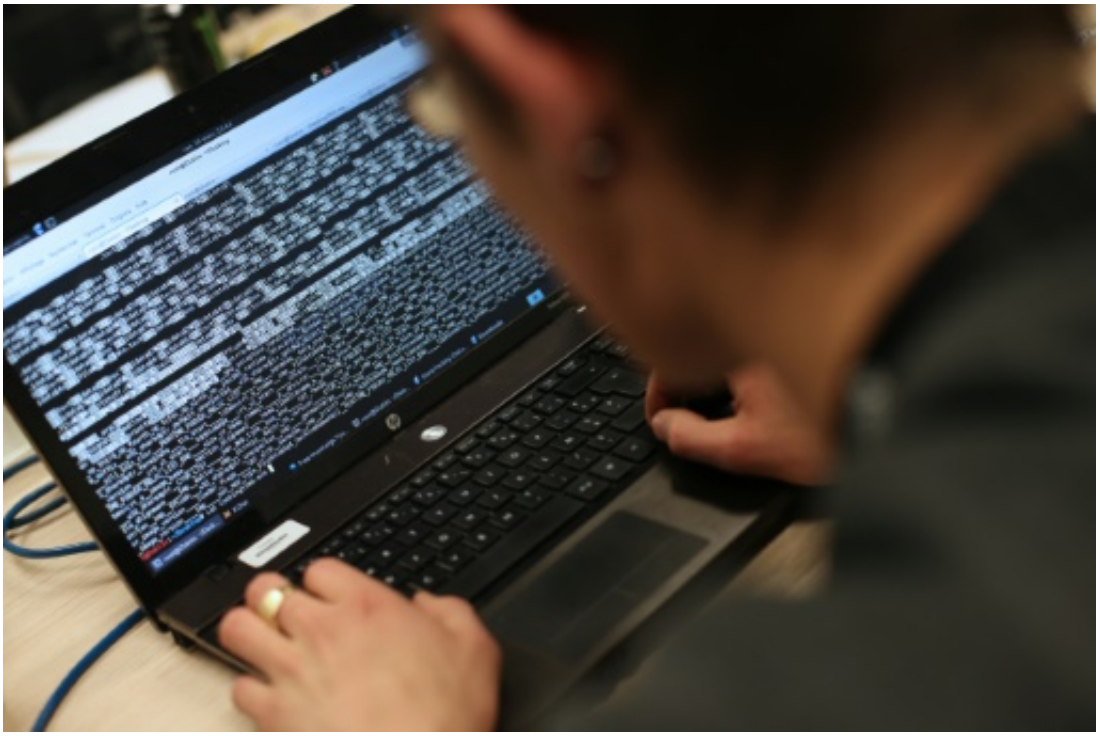
Bank hacks raise fears for financial sector

July 25 2016, by Rob Lever



Banks in Bangladesh, the Philippines, Vietnam and Ecuador have been victimized over the past year in the attacks on the global interbank service known as SWIFT

A series of spectacular cyber attacks against banks, resulting in the theft of tens of millions of dollars, has heightened fears for an industry becoming an increasingly attractive target for hackers.

Banks in Bangladesh, the Philippines, Vietnam and Ecuador have been victimized over the past year in the attacks on the global interbank

service known as SWIFT, and some analysts expect more attacks to become public.

After news of the $81 million heist from Bangladesh's central bank became public in May, SWIFT said the incident was "not a single occurrence, but part of a wider and highly adaptive campaign targeting banks."

Since then, officials said banks have also been hit in the Philippines and Vietnam.

Meanwhile Ecuador's Banco del Austro claimed in a lawsuit that hackers made off with more than $9 million through fraudulent SWIFT transfer requests.

Cyber security specialists say these attacks are likely just the tip of the iceberg, and expect more revelations.

"Cyber criminals are no longer targeting grandmothers at home for small amounts, but going directly where the money is," said Juan Andres Guerrero-Saade, a researcher with the security firm Kaspersky.

Guerrero-Saade said it's not clear where the attacks are coming from, but that the hackers are using techniques similar to those developed for cyber espionage.

"I don't think this implies it's nation-states, it's more of an evolution," the analyst said. "It's criminal actors taking on some of those techniques."

Kaspersky researchers last year uncovered a hacker group which targeted banks in Eastern Europe, estimating losses totaling up to $1 billion.

Dan Guido, cofounder of the security firm Trail of Bits and former hacker-in-residence at New York University's engineering school, said the recent security breaches are not surprising.

"I didn't think it would take this long," Guido said.

"There are a large number of attacks like this possible if someone has the resources to do it."

Guido said a relatively small team of determined hackers could carry out the kind of hacks that went through SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, a Brussels-based network which is used by more than 11,000 financial institutions in 200 countries.

More aggressive security

The blame, Guido said, rests squarely with SWIFT for failing to bolster its software or require more secure hardware.

"It's clearly within their control to have prevented incidents like this," Guido said.

"They could have had more aggressive security requirements, they could have had protective hardware."

On July 11, SWIFT announced it had hired cyber security firms BAE Systems and Fox-IT while creating its own security intelligence team in an effort to thwart attacks.

In the United States, concerns have been raised among officials, industry leaders and lawmakers about potential threats to banks from hackers.

Data breaches in the past affected some tens of millions of JPMorgan Chase customers, and accounts from financial giant Morgan Stanley. And a congressional report in June found "major data breaches" at the Federal Deposit Insurance Corporation.

Senator Tom Carper last month asked the Department of Homeland Security for a briefing for an investigation into vulnerabilities of the US financial system.

The American Bankers Association in July joined with other financial and security organizations to warn of possible risks.

"While recent events targeted national financial institutions with access to a global payment network, financial institutions should assess the risk of all critical systems to ensure appropriate controls are in place," said the warning, calling for a series of new controls and safeguards against cyber attacks.

Doing reconnaissance

Christiaan Beek of Intel's McAfee Labs said the hackers that targeted SWIFT were well organized and resourceful.

"We can see that the attackers have done their reconnaissance properly and may have used an insider to get the details they needed to prepare their attack," Beek said in a blog post.

"The attackers have a very good understanding of the SWIFT messaging system and how to manipulate the system to prevent the detection of their fraudulent attempts of transferring the money."

Researchers at the security firm Symantec concluded that malware used in the bank hacks shared code with that used in the massive 2014 cyber

attack against Sony Pictures.

Guido said it is entirely plausible that US banks could face similar attacks.

"I don't see why it can't happen here," he said.

"There are a lot of smaller banks that don't have expertise and guidance to protect their interconnections."

Guerrero-Saade said a key part of staying ahead of hackers is sharing information about threats to enable security solutions, since many companies fear disclosure would hurt their business.

"Sadly most companies don't tend to be very forward looking, they think that if they don't sound the bell themselves no one will find out," he said.

"It's much better for us to get ahead of this as an international community."