Bangladesh hack illustrates rising sophistication of attacks

SWIFT CEO Gottfried Leibbrandt has announced a number of measures that it is hoped will better safeguard financial transactions in the future, following the penetration of the SWIFT network that saw cyber criminals make off with substantial amounts of money, marking a new stage of sophistication in cyber attacks against financial institutions. David Ferbrache, Technical Director, Cybersecurity at KPMG in the UK, shares his opinion on the threat facing the global payments network, the present limitations and the weak links in international anti-money laundering regimes that enable criminals to cash-out their ill-gotten gains.

The weakest links

The theft of US$81 million by cyber criminals from the central bank of Bangladesh[1] has prompted the Society for Worldwide Interbank Financial Telecommunication ('SWIFT') to call for tighter antifraud controls and closer cooperation among its 11,000 members. This initiative is welcome, but the measures announced by SWIFT can't guarantee the security of global payments. The Bangladesh Bank heist shows the ability of criminals to strike at the global payments system, in their attempt to get away with US$1 billion. Unless improvements are made, it's only a matter of time before we see them, or someone else, succeed.

To reduce the risk further would require a much wider and more coordinated effort among banks, payment networks, regulators and governments to strengthen security, especially among the weakest links in our financial infrastructure. The vulnerable links include any and all parts of the system where fraud controls are weak and data security is at risk. We may expect the largest global banks to implement comprehensive security controls, but this may not be the case for all members of our community. Smaller banks, banks in emerging markets, new entrants to the financial community, and some government institutions may face greater challenges. All are connected in some way to the global financial markets.

The Bangladesh case demonstrates that cyber criminals are continuously searching for parts of the financial system where there are gaps in defences, where security controls can be bypassed, and where insiders may be prepared to collude in perpetrating fraud. If members of the SWIFT payments network follow through and significantly tighten their safeguards against cyber attack, criminals will focus their efforts elsewhere on the financial system. They have shown they are able to compromise not just commercial banks but a central bank.

As SWIFT CEO Gottfried Leibbrandt told the European Financial Services Conference in Brussels on 24 May 2016, the fraud at Bangladesh Bank "will prove to be a watershed event for the banking industry; there will be a before and an after Bangladesh." The question, of course, is what happens after.

A systemic risk

Leibbrandt told the conference in Brussels that in the event leading to the theft from Bangladesh Bank, SWIFT's network, software and core messaging services were not compromised. This is reassuring, but small consolation for the 11,000 institutions that are members of SWIFT, because it is clear that thieves don't have to attack SWIFT's core systems to exploit weaknesses in the systems that feed in and out of SWIFT's network. Instead, the penetration occurred at Bangladesh Bank, a member of the SWIFT network, and at other banks.

Investigators are continuing to examine what happened, and new details are likely to continue to emerge. What we do know is that the attackers opened a number of accounts at Rizal Bank Philippines in May 2015. They then conducted reconnaissance to identify targets to gain access and penetrate the banking system.

In early February, the attackers made 35 fraudulent payment requests to the New York Federal Reserve from

1. https://www.kpmg.com/Ca/en/services/Advisory/RiskCompliance/Cyber-Security/Documents/KPMG-Cyber-Watch-Threat-IntelligenceAlertFINAL.pdf

Bangladesh Bank's server, totaling US$951 million. Fortunately for the bank, vigilance by recipient banks and a spelling error in a request stopped the bulk of the transactions and only five of the 35 were authorized and paid. The criminals had planted malware that modified the SWIFT Alliance Access Server software to bypass authentication checks and cover its tracks to avoid detection.

At Bangladesh Bank, there was no indication of trouble and no alerts of an intrusion until 5 February 2016, when the bank realized there were no SWIFT printouts that day. A full day went by and then the transactions were printed out, revealing the suspicious activity. Stop-payment orders were issued on 8 February 2016. Nevertheless, on the following day, the branch manager of Rizal Bank allegedly approved the withdrawal of US$81 million.

In the ensuing investigation, it came to light that at least two, and possibly more, other cases had recently occurred where fraudsters used similar methods to penetrate financial institutions through the SWIFT network, but got away with lesser amounts. One of the cases involved a commercial bank in Vietnam.

As Leibbrandt explained in his speech, "The banks were compromised, credentials to payment generation systems were obtained to send fraudulent payments and the statements/confirmations from their counterparties were obfuscated." The problem is twofold: first, when banks lose control of access to their payments channels, the possible loss of assets could threaten their existence; second, the financial system is tightly interwoven and operates on the basis of trust, which could disappear in the event of a significant penetration by a criminal organization.

Game changer

To understand what happened, a number of points are worth noting:

— The cyber attack on Bangladesh Bank marks the culmination of efforts by criminal groups to penetrate the global payments banking system. The precision of the targeting, the care taken in preparations, and the sums involved mark a new stage of cyber attacks on financial institutions.

— The group that carried out the theft of funds from Bangladesh Bank sought to extract the cash from places where it was feasible to launder large amounts of cash. The money withdrawn from Rizal Bank entered casinos in the Philippines that are not subject to comprehensive anti-money laundering controls.

— The timing was important. The thieves exploited the difference in the timing of weekends in Bangladesh and New York, so that queries from one country went unanswered in the other. And the heist occurred over Chinese New Year, when Filipinos go on holiday, leaving only skeleton staff to monitor bank transactions.

— The scale of the SWIFT payments network and the systems that connect to it makes it difficult to prevent unauthorized penetration by a determined hacker. There are 11,000 member institutions in more than 200 countries and therefore millions of employees, both present and former, who use, or have used, the system and understand aspects of its operation.

— In 2015, a total of more than 6 billion messages were relayed through the network among members, nearly 17 million a day. Such a high number makes it extremely difficult to spot anomalies without the use of data analytics to monitor all transactions.

— Payments made by one institution to another are typically highly automated; straight-through processing is becoming increasingly commonplace. A sufficiently determined cyber criminal will find a way to defeat fraud controls and minimize delays in 'cash-out.'

— All 11,000 institutions enjoy access to SWIFT, irrespective of the relative level of their internal data security. The ability of the network to withstand a cyber attack is only as great as the weakest link in the network. Criminals will inevitably target those institutions with the weaker controls and lower levels of security.

— SWIFT's core messaging services were not compromised, but the systems used by the institutions were penetrated. As Leibbrandt pointed out, SWIFT "cannot secure our customers' environments and cannot assume responsibility for that." SWIFT is a global cooperative owned by its members, but it is not practical — at least for now — for all members to operate at the highest level of data security.

> The key is to identify just how cyber criminals can cash-out and monetize the access they achieve to our global financial systems, including the payment and clearing systems at the heart of our financial world.

Beyond Canute

In his speech, Leibbrandt outlined five ways that SWIFT intends to safeguard financial transactions better in the future:

1. Demand more information from SWIFT's customers and share it back with the community.
2. Harden security requirements for customer-managed software to protect customers' local environments.

3. Enhance guidelines and develop security audit frameworks for customers.
4. Support banks' increased use of payment-pattern controls to identify suspicious behaviour.
5. Introduce certification requirements for third party providers.

These measures will certainly go some way towards improving the security of bank transactions round the world. They are a welcome step in the right direction, but they need to go further. In the Bangladesh case, it was the central bank that was compromised. It also regulates the banking system, raising doubts about the ability of some country regulators to demonstrate the security precautions that they themselves expect of the banks they regulate. Who watches the watchmen?

Cyber criminals will continue to look for the weakest entities in the financial system. Will these entities be brought up to the standards of the stronger ones, as a result of the changes envisaged by SWIFT's CEO? Other measures should be taken to identify the weakest links in the chain of financial transactions, by establishing improved regulatory baselines for payments security and undertaking a risk-focused assessment of the participants' ability to manage security and prevent fraud.

A particular focus of the assessment should be the skills and resources available at each institution. Some members of the SWIFT network lack the knowhow to safeguard their assets from the sophisticated cyber attacks we are now seeing. And many have limited, or no, staffing of their security and fraud teams at weekends or on public holidays. Criminal gangs do not take the day off. Indeed, they are more likely to be active when banks' guards are lowered.

SWIFT is probably not in a position to demand that the licenses of all its banking members be contingent on their meeting certain rigorous standards of cyber security. But worldwide banking regulatory bodies such as the Bank for International Settlements ('BIS') should promote a higher global baseline.

In addition to these measures, governments around the world must do more to eradicate havens of money laundering and potential gaps in the international antimony laundering regime. Ultimately, the more difficult it is to cash-out the proceeds of crime, the lower the incentive to commit it. This is difficult to achieve, but we need to see the same level of political resolve to crack down on money laundering that we have seen developing on tax avoidance.

Global answers to a global problem

By focusing on the problems encountered by SWIFT, we risk losing sight of the wider issues faced by the global financial system that are highlighted by the Bangladesh Bank case. The key is to identify just how cyber criminals can cash-out and monetize the access they achieve to our global financial systems, including the payment and clearing systems at the heart of our financial world.

Then the financial community, both public sector and private, needs to work together to introduce a range of measures, consisting of fraud controls, data analytics and other security strategies for each of these key systems and the gateway systems that communicate with them. Each of these systems is a separate organisation with its own rules, but to a criminal group, they all present opportunities to move money around. If this does not happen, we run the risk that a single weak link in one payments system could undermine confidence in the entire global financial framework.

Contact:

David Ferbrache
Technical Director,
Cybersecurity
KPMG in the UK

Designed by Evalueserve.
Publication name: Bangladesh hack illustrates rising sophistication of attacks
Publication number: 133601-G
Publication date: August 2016