SSEI
Sanjay Saraf Educational Institute Pvt. Ltd.
A positive NPV Training Center

CA FINAL

RISK MANAGEMENT

IN-HOUSE

CASE STUDY SERIES

-By Sanjay Saraf Sir

Case Study 18 Questions

Powered By -

ULURN
KNOWLEDGE IN DEPTH

SSEI QFORUM

Bangladesh Bank Heist: Lessons Learned

SWIFT is a Belgium-based cooperative of 3,000 organizations that maintains a messaging platform used by banks, mostly in Europe, to transfer money across borders, often in real time.

"It was the bank's systems or controls that were compromised, not the software," says William Murray, an independent payments security consultant. "The SWIFT software behaved as it was intended to, but was not operated by the intended person or process. This is a bank problem, not a SWIFT problem."

The attack waged against Bangladesh Bank, the nation's central bank, in February was similar to account takeover attacks waged against commercial customers, Murray contends. "This is an account takeover attack, similar to those that the industry has been dealing with for years," he says. "However, it is the account of the bank with SWIFT, rather than that of the bank's customer, that is being taken over. ... Banks should be using the very same controls over their own systems that they expect of their own customers. Good security is good security."

Banks should conduct SWIFT transactions only on computers that are isolated from other devices on their networks, says Sean Sullivan, an adviser at the security firm F-Secure. "It should be a dedicated computer for its single task," Sullivan says. That's the same advice banks have for years been giving to their commercial customers who schedule wire transfers and ACH payments online.

"The malware was able to be installed on the SWIFT software computer because the attacker was in Bangladesh Bank's network with access - presumably with enough access to override any locally installed security software if there was any," Sullivan adds.

Shirley Inscoe, an analyst at consultancy Aite, says the breach likely involved an insider connection. "While hackers can successfully access many systems without insider assistance, almost certainly insider knowledge of how the system operates was used to overcome the fraud detection controls," she says. "This knowledge could easily have come from a current employee at SWIFT or Bangladesh Bank."

Malware Methods

The malware used to compromise a computer used for SWIFT transactions was designed to hide traces of fraudulent payments from the bank's local database collections, according to technology consultancy BAE Systems Applied Intelligence.

What's more, once money is transferred via SWIFT, it's typically not reversible, which makes this attack even more clever, Murray says.

"Keep in mind that SWIFT is a messaging system that banks use to communicate with correspondent banks," he says. "Multiple banks and transfers may be involved in completing a transaction, all taking place within seconds. And because multiple banks and accounts may be involved, by default, the transfers are not reversible when disputed."

This kind of "straight-through" payment process gives fraudsters an advantage, says Tom Kellermann, CEO of security firm Strategic Cyber Venture. Banks should be bracing for more of these types attacks, especially as the U.S. moves toward faster, real-time payments, he advises.

"Straight-through processing empowers the cybercrime community. SWIFT has been over-reliant on PKI [public key infrastructure] to protect the payment system for years. Private keys are being compromised as credential theft explodes."

SWIFT Taking Action

In a statement provided to Information Security Media Group, SWIFT notes that it is aware of the risks and is taking steps to help banks shore up security.

"We understand that the malware is designed to hide the traces of fraudulent payments from customers' local database applications and can only be installed on users' local systems by attackers that have successfully identified and exploited weaknesses in their local security," the statement says. "We have developed a facility to assist customers in enhancing their security and to spot inconsistencies in their local database records.

"However, the key defense against such attack scenarios remains for users to implement appropriate security measures in their local environments to safeguard

their systems - in particular those used to access SWIFT - against such potential security threats. Such protections should be implemented by users to prevent the injection of malware into, or any misappropriation of, their interfaces and other core systems."

Multiple Choice Questions

1. Which of the following is TRUE about the SWIFT (Society for Worldwide Interbank Financial Telecommunication) case study?

A. The 2015-16 cyber attack (aka, hack) demonstrated that the SWIFT network was unreliable and it was subsequently phased out

B. The 2015-16 cyber attack (aka, hack) successfully exploited vulnerabilities to achieve the theft of about USD 81.0 million

C. The 2015-16 cyber attack (aka, hack) was an unsuccessful attempt to steal money, and it demonstrated the SWIFT network is essentially impervious to attacks

D. The 2015-16 cyber attack (aka, hack) was a fictitious news account but the negative press nonetheless shook confidence sufficiently in the network that transactions ground to a halt for several weeks

2. Which of the following statements is correct regarding cyber risk?

A. Cyber risk is only a danger for banks.

B. Cyber risk must be retained and mitigated with internal resources.

C. Cyber risk is becoming less of an issue due to the impact of regulation.

D. Cyber risk involves the potential for loss resulting from a technology-related breach.

3. A type of malicious software designed to lock or encrypt access to a computer system until a sum of money is paid is called :

A. DoS

B. Ransomware

C. Phishing

D. Malevolent Attack

4. **Which of the following can lead to malevolent attack on system of an institution that can lead to complete or partial data loss, of customers, accounts and of past financial transactions**

A. Malevolent Attack

B. Phishing

C. Intellectual Property Risk

D. Ransomware

5. **Which of the following is not a factor in securing the environment against an attack on security?**

A. The education of the attacker

B. The system configuration

C. The network architecture

D. The business strategy of the company