Article Summary:

I chose the cyberattack on Iran’s Sepah bank. This attack led to the compromise of 42 million customer records (which is around 12 terabytes) on June 17,2025. Bank Sepah is a state-owned bank and one of the largest financial institutions in Iran and it has a strong military tie. This bank was attacked by a pro-Israel, hacktivist group called “Predatory Sparrow” or Gonjeshke Darande. The motivations are targeting Iranian infrastructure like steel mills, fuel systems, the country’s rail system network, and more. Due to the severity of the attack customers couldn’t access accounts, bank branches had to close, payment processing was down, and the website was offline. The attackers said that it targeted the bank due to “circumvented international sanctions and used the people of Iran’s money to finance the regime’s terrorist proxies, its ballistic missile program and its military nuclear program.”

CIA Analysis

Confidentiality –

Confidentiality was attacked because the hackers stole the data from Bank Sepah. Although, there was no reporting of the data being stolen or misused one’s information is still at risk. The goal of the hacktivists was to delete the data. If I banked with Bank Sepah, I would need them to verify that my information was not taken. These hackers could one day decide to post the data.

Integrity –

The hackers claimed they deleted the data, but one can never trust the word of a bad guy. If they did delete the data, it would directly attack the integrity of the data. The destruction of records, transactions, and balances undermines the reliability of the databases they could’ve been in. If I was banking with them, I would really have questions over my money and if all transactions were properly documented so that my money wasn’t affected. I especially would have questions about the information of my account being spread via online platforms.

Availability-

The availability was especially attacked. The bank’s website, brick & mortar locations, and processing payments were offline. This is a direct effect on the availability of Bank Sepah, this is what makes a bank functional. The fact that the hacktivists could stop the Bank from fully functioning should alarm the cybersecurity team. The vulnerabilities were very clearly exploited and should’ve been found before the hackers could even attempt to attack the bank.

Article Link:

<https://cyberscoop.com/iran-bank-sepah-cyberattack/>