CyberProof®
A UST Company

Better Security, Together.

The True Cost of Cyberattacks on the Financial Sector in 2024

Five examples of the vulnerability of the finance industry against cybercrime

> The financial sector is uniquely exposed to cyber risk. Financial firms—given the large amounts of sensitive data and transactions they handle—are often targeted by criminals seeking to steal money or disrupt economic activity. Attacks on financial firms account for nearly one-fifth of the total, of which banks are the most exposed.
>
> IMF, April 2024

1 Ransomware attack against Prudential impacts 2.5M people

In February 2024, financial services company Prudential disclosed a ransomware attack that they believed impacted 36,000 people. In July, this was updated to 2.5M.

The cost of the breach

While there is no sign that Prudential paid a ransom, impacted customers have been offered 24 months of free credit monitoring, and due to a 52-day delay in notifying consumers, a class action suit is in progress.

2 Close to 300 banks in India are forced to take payment systems offline

In July 2024, customers of cooperative and regional banks across India were impacted by a ransomware attack on C-Edge Technologies, a provider of banking technology systems.

The cost of the breach

For multiple days, customers of almost 300 banks were unable to process transactions, including withdrawing cash from ATMs, and making online payments via UPI or RTGS. This could lead to a serious erosion of customer trust and financial services' reputation.

3 The Complete Blackout of EquiLend's Electronic Trading Systems

In January and February 2024, the Wall Street stock-lending platform was forced to take many client-facing services offline after a ransomware attack by LockBit.

The cost of the breach

EquiLend's NGT platform alone processes more than $2.4 trillion in transactions monthly, and services were offline for close to two weeks. In addition, in March 2024, EquiLend disclosed that employee data had been compromised, including names, dates of birth and social security numbers.

4 A Run of Loan and Mortgage Companies Hit by Hackers

Between October 2023 and January 2024, several loan and mortgage companies were targeted by cyberattacks, knocking services offline and causing significant financial harm.

The cost of the breaches

Loan giant Mr Cooper had 14M customers' data stolen, with estimated costs at least $25M. Fidelity National Financial, one of the largest home insurance providers in the U.S. had services taken offline for more than a week because of BlackCat/ALPHV ransomware. LoanDepot reported data of close to 17M customers stolen, and say recovery is likely to cost between $12M-$17M.

5 The World's Largest Bank Targeted by LockBit

In November 2023, the US unit of the ICBC in China, the world's largest lender, was hit by a LockBit ransomware attack — freezing its ability to clear trades in the U.S.

The cost of the breach

The business disruption of the ransomware attack was so severe that even corporate email was offline. On top of the cost of downtime, ICBC paid BNY Mellon $9B for unsettled trades, and hired a cybersecurity firm to help get services back up and running. Additionally, according to LockBit — IAC paid the ransom.

Looking to protect your customers and their data, and prepare a ransomware readiness plan ahead of time? **Speak to one of our cybersecurity experts.**