Banking Cybersecurity Threats Overview – 2024

Advanced persistent threats

Advanced persistent threats (APTs) refer to organized campaigns that establish a long-term presence inside a bank network. The intruders then steal sensitive information or manage internal takeovers.

Such attacks are complex. They often use a mix of trojan and backdoor injections, and once inside, fraudsters can perform counter-security measures that evade detection.

This tactic is unique to the sophistication of bank networks, and when successful, it may lead to all manner of financial fraud. A recent example includes the Sidewinder APT, which has targeted governments and financial institutions worldwide.

Supply chain attacks

The digitization of banking allows numerous third-party services to integrate with secure bank systems. For example, fintech software development has allowed neo-banks to earn a competitive service edge compared to traditional banks. Such integrated networks offer efficient service convenience for consumers.

However, this also creates vulnerabilities. Cybercriminals can now target vendors inside your supply chain that have weaker security. For example, Okta reported three recent data breaches due to supply chain attacks. Criminals executed the hacks on the authentication service through GitHub repositories.

Phishing and social engineering attacks

Human error remains a critical weak point with IT security in banking. Bad actors continue to use scams that trick employees and customers into providing personal information (especially after the pandemic). This is a type of identity theft.

For example, many fraudsters pose as a bank, high-level representatives, or the government to gain credit card data. Others use phishing emails or messages that contain malicious links. Spoof websites that mirror secured bank web pages are also common ploys. When Silicon Valley Bank made the headlines due to its impending insolvency, scam domain names with similar URLs spiked.

Social engineering in all its forms remains a prominent risk factor that your cybersecurity team should take steps to address.

Unencrypted data

Usually, cybersecurity teams scramble all data with encryption. Only someone with the appropriate key can reassemble the data, making it far easier and safer to transfer. Even if a fraudster steals the information, the data is useless without the key.

Hackers expend immense effort attempting to steal data the minute it is left unencrypted within a banking server. Most recently, a cybersecurity researcher found an entire unencrypted database with sensitive customer information held by Canadian fintech platform NorthOne.

Ransomware attacks

Ransomware remains a top security threat for banks. Criminals steal and encrypt financial documents that lock clients out of their own systems. In many cases, the

programs can paralyze bank services for extended periods of time. To unfreeze the services, you must pay the ransom demanded by the criminals.

Ransomware remains a big problem for banks, as downtimes frustrate users and harm public reputations. Just this year, the Lockbit Ransomware seized the internal operations of the Banco de Venezuela, the largest financial institution in the country.

Major cybersecurity risks your bank might be ignoring

As cybersecurity in the banking industry evolves, so do bad actors. Fraudsters exploit the weak points in new technologies and attempt novel strategies. The banking sector should prepare for the following risk factors trending in 2024:

Emerging tech

Financial institutions experience a far greater surface area of attack with the introduction of new technologies. Examples include artificial intelligence, blockchain, and cryptocurrency.

Machine learning and smart contracts are useful and disruptive solutions for those with a well-prepared defense posture. However, both technologies are in their early adoption stages and still suffer from code errors and algorithm weaknesses that intelligent hackers can exploit. It's a good idea to update legacy systems with new services, but only after you complete extensive cybersecurity risk assessments.

Cloud vulnerabilities

Cybersecurity in the banking industry has committed to cloud solutions. All internal operations improve once a business adopts flexible cloud-based systems, but the migration does include risks. For example, cloud services offer rigid security controls, but those efforts are useless if misconfigured. There is also a shared responsibility between providers and banks — most institutions now need new cloud security regarding data leakage, access management, and privilege abuse.