Understanding cybersecurity management for FinTech: cybersecurity threats in FinTech (Article 3) - IT World Canada

November 1, 2021

With a plethora of digital wallet methods, financial cyber risks such as fraudulent transactions, extortion, denial of service attacks, and credit card fraud have become frequent. These cyber-attacks are capable enough to cause systemic risk to the financial sector. Some of the most prominent cyber-attacks that the financial sector has witnessed so far have impacted critical economic infrastructures. These attacks have the potential to deliberately destroy hardware, and to compromise sensitive business data to adversely impact services.

Cybersecurity threats impact almost all the components in the FinTech ecosystem. They may pose potential exposure to various financial institutions that use technology, FinTech startups, and financial customers in the FinTech ecosystem. Technology developers also need to be aware of potential cybersecurity threats

that can exercise vulnerabilities and flaws in the technology that they are developing.

This article uncovers various cybersecurity threats in FinTech and provides deep insights into categories and actors causing those threats. It also introduces the threat modelling approaches used by financial institutions to mitigate the countermeasures of these threats. The content in this article is based on the extensive research work behind our book titled *"Understanding Cybersecurity Management for FinTech"* published by Springer this year.

Cyber threats

FinTech has witnessed various types of cyber threats, including malware, data breach, denial of service, cyber fraud, and phishing. Data breach and distributed denial of service (DDoS) are the two most common cyber-attacks that have been recorded on a regular basis in the timeline of cyber risks and threats on FinTech across the globe. Figure 1 below highlights the reported cyber-attacks and threats that incurred major monetary losses to financial institutions and banks between 2007 and 2019. It is evident that cyber threats pose severe risks to FinTech over the years.

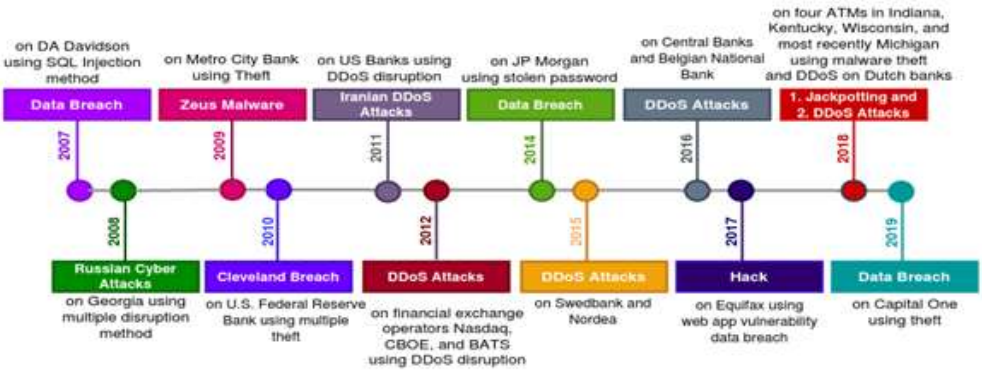

Figure 1: Timeline of cyber threats on FinTech across the globe

Cyber-attacks have targeted financial institutions and banks all over the world. Some recent cyber threat attempts include: hijacking famous Twitter accounts for bitcoin (US), Scotiabank data breach (Canada), ransomware attacks (US), GoldenSpy malware in tax

software (China), DDoS attacks (Europe), dForce cryptocurrency (China), and DDoS extortion (Australia).

Threat categories

FinTech companies face the most prevalent cyber threats. This section defines paramount cyber threats to FinTech startups.

- **Malware:** Malware is malicious software specially designed to disrupt, damage, or gain unauthorized access to a computer system to steal sensitive information. Malware can be classified as: Adware, Ransomware, Riskware, Scareware, Spyware, Trojan horse, Virus, Worm, and Zero-day.
- **Adware:** Adware represents advertisement malware. It is a malicious application that throws unwanted advertisements on the user screen. Adware lures the user towards flashing advertisements that offer lucrative products and attract them to click on the advertisement.
- **Ransomware:** Ransomware is malware that encrypts files and directories on the machine to make them inaccessible to users. It asks for a handsome amount of ransom to provide the decryption key that is used to unlock the data.
- **Riskware:** Riskware is a legitimate program that poses potential risks to the security vulnerabilities on the device. Although it is a genuine program, it is used to steal information from the device and redirect users to malicious websites.
- **Scareware:** Scareware is a fear coaxer that raises fear in users' minds to encourage them to download or buy malicious apps.
- **Spyware:** Spyware is malicious software that can steal sensitive information once installed on the device. The data collected by spyware is passed to advertisers, external agencies, or firms.
- **Trojan:** Trojans are sneaky impersonators that behave like legitimate programs. They can hide in the background and steal information from the device.
- **Virus:** Virus is a computer program that replicates itself by changing other programs and inserting its own code.

- **Worm:** Worm is a computer program that does not require a host program. It replicates itself to spread to other computer systems. A worm uses the target machine to infect other machines on the network.
- **Zero-day:** Zero-day is a vulnerability that is unknown to the security community. Zero-day is referred to as the duration in which the vulnerability is not known to people and a malicious program is developed to exploit the vulnerability. Once the vulnerability is made public, vendors develop the patch to fix it.
- **Data Breach:** Data breach is the act of leaking sensitive or confidential data either intentionally or unintentionally to any untrusted party.
- **Denial of Service:** Denial of Service (DoS) is a targeted attack launched against a computer system, server, or network to make the services unavailable to legitimate clients.
- **Distributed Denial of Service:** Distributed Denial of Service (DDoS) is one of the lethal and targeted attacks involving multiple attackers and multiple compromised systems.

Threat actors

Threat actors are the unauthorized individuals or groups behind launching cyber-attacks on any organization. Although the alleged personnel remain the same for every organization, a special workforce of attackers is observed for financial institutions. Some of the prominent threat actors identified based on the history of cyber-attacks targeting the financial sector are listed below:

- **Malicious insiders:** These are authorized people who have the rights and permissions to access, read, write, and transfer critical private and proprietary data of a financial institution, especially in banks. According to the IBM's Cost of a Data Breach report 2020, the average cost of data breaches is $6.71 million. It includes both system glitches and human error. Additionally, the average cost of cyber incidents, across different sectors, is $4.37 million. In HSBC bank's internal fraud case in 2008, a clerk at its headquarters in

London fraudulently wired €90 million to accounts in Manchester and Morocco. The clerk used passwords stolen from his colleagues to execute these transactions. However, the clerk was later arrested and was sent to jail for nine years.

- **Hacktivists:** Hacktivists perform politically or religiously motivated activities to misuse a computer system or network. The act of performing such activities is called hacktivism. Hacktivists are also called hackers in simple terms. They act in groups and collaborate to coordinate a politically acclaimed cyber-attack on major financial institutions of the country. In a related incident in 2016, some anonymous hacktivists took down the website of Bank of Greece, and central banks of Mexico, Panama, Kenya, Bosnia, and Herzegovina by launching DDoS attacks.
- **Cybercriminals:** Cybercriminals are individuals or groups of techno savvy professionals who use technology to perform malicious activities on digital systems or networks to steal sensitive data for financial gain. They are popular for accessing underground markets found on the dark web to trade illegitimate goods and services such as weapons, banned medicines, adult content, and narcotics. Cybercriminals infiltrate computer systems with the intention of finding useful information with which to launch targeted attacks. An international group of cyber criminals used GozNym malware to steal $100 million from over 40,000 victims, including bank accounts, law firms, small businesses, international corporations, and nonprofit organizations in 2019.
- **Nation-states:** Nation-state actors or state-sponsored actors are well funded and sophisticated. They are sponsored by a government entity. One of the recent nation-state attacks was the NoPetya ransomware outbreak in 2017 that targeted Australia, Europe, Ukraine, and the US. NoPetya is considered the fastest propagating malware ever.
- **Cyber terrorists:** Cyber terrorists are involved in carrying out malicious activities to shut down critical infrastructure of the target. These activities fall under cyber terrorism, which is

considered as the new cyber war. Researchers classify NoPetya and WannaCry ransomware as acts of cyber terrorism.

- **Script kiddies:** Script kiddies are beginners or unskilled people who are lured to cybercrime activities.

Threat modelling

FinTech threat modelling follows a structural approach to identify, categorize, and analyze cyber threats. The primary objective is to accurately identify potential threats that can exploit vulnerabilities in the FinTech institution and result in huge financial losses. It attempts to reduce the vulnerabilities and their impact on the FinTech institution. It can be performed as a proactive or reactive measure.

A proactive threat modelling approach is also called a defensive approach that aims to defend the FinTech institutions against cyber-attacks. It is based on predicting threats so that early warnings can be issued, and resources can be secured. However, it is impossible to predict all cyber threats in real-time.

A reactive threat modelling approach protects against adversarial attacks by taking appropriate actions to prevent a cyber threat. It is also known as the adversarial approach, and includes ethical hacking and penetration testing techniques.

FinTech institutions focus on assets, attackers, or software to model threats. A selection of an appropriate structural approach entirely depends on the type of FinTech, its size, and investment in business.

What's next

This article introduces cyber threats in the FinTech industry and answers the question: why are we afraid of cyber threats? It puts forward various threat categories, threat actors, and approaches to model threats. The next article of the *Understanding cybersecurity management for FinTech* series explores cybersecurity vulnerabilities and risks in FinTech.

Would you recommend this article?

+4

0