ITWC BLOGS

Privacy & Security

Understanding cybersecurity management for FinTech: security issues on financial market infrastructures (Article 5)

By **Gurdip Kaur and Arash Habibi Lashkari** - February 1, 2022

Financial market infrastructure (FMI) serves as the backbone of financial markets. It allows financial transactions to take place between people, financial institutions, and businesses in a cheaper and more efficient manner. It is the key component between financial institutions that exchange payments, securities, and derivatives. It allows customers and financial firms to purchase goods and services safely. It strengthens financial stability and economic growth by recording, clearing, and settling monetary and other financial transactions.

Simple examples of FMI include depositing salary into an employee's account, taking cash from an ATM machine, and paying for online purchases. FMIs also play some other essential functions, such as transferring shares between traders and the stock market, helping banks borrow money from other banks and financial institutions in the market, and lending and borrowing loans to buy houses and invest in the business. FMIs played a pivotal role in the financial crisis of 2007-2009. They acted as a stabilizing force behind settling uncertainty in monetary transactions.

This article introduces the concept of financial market infrastructures and several types of FMIs. It identifies various security issues in central counterparties. 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.

Introduction to FMI

Financial market infrastructure is defined as a multilateral system designed to record, clear, or settle payment systems among participating financial institutions. Apart from handling payment systems, it also includes settlements, securities, derivatives, or other financial transactions. The participating financial institutions are referred to as buyers and sellers. FMIs establish common rules and procedures for participating entities that consider a specialized risk management framework to deal with risks. It ensures financial stability and economic growth by effectively managing risks that may incur in the financial system. A complete structure of FMI along with essential components is presented in Figure 1.

1. Payment systems

A payment system is a set of rules and procedures used to transfer funds between participating entities. It operates based on an agreement between the entities and the operator. It enables lending and repayment of money, payments for goods and services offered, salaries, and benefits for the general public. It is generally categorized as either a foreign exchange transaction or a retail payment system. Foreign exchange (FX) transactions are the most liquid sector of payment systems in the financial market. It primarily deals in international trade and investments through exchange rates of currencies and transfer of funds. The types of payment transactions covered by payment systems include domestic card payments, credit transfers (internet and mobile payments), direct debits, and inter-bank transactions.

Figure 1: Essential components of FMI

2. Central securities depositories

A central securities depository holds a security account for fund transfer either in a certificated or uncertificated form. It plays a key role in ensuring the integrity of security issues. It may maintain a record of legal ownership for security. The functions performed by a central security depository may vary depending upon the jurisdiction in which it is operating. It is responsible for the electronic accounting of assets and services, fund transfer, and security transfer system. It includes stock exchanges, Over-The-Counter (OTC) derivatives, equities, and money market instruments.

3. Securities settlement systems

Security settlement systems are a critical component of financial market infrastructures. They act as an intermediator between borrowers and lenders to secure the flow of funds, and maintain their security portfolios. They allow the transfer of payment, either free of cost or against payment. When the transfer is made against a payment, delivery of the security is taken care of, if and only if payment is made. They also ensure the safekeeping of securities by providing additional security clearing and settlement instructions. To summarize, they provide security to the flow of funds against a settlement between the trading parties.

4. Central counterparties

A central counterparty acts as an intermediator by acting buyer to the seller and vice versa. It interposes itself between counterparties to financial contracts traded in the financial market. It is also called clearinghouses. Central counterparties (CCPs) place themselves between buyer and seller to reduce the complexity of trade. Once the buyer and seller finish a transaction, a post-trading system ensures that all trade agreements are effectively enforced by matching all buy and sell orders in the market (clearing), transferring securities under each contract (settlement), and safekeeping securities (custody). Before central counterparties were used in trade, all the participating entities (buyers and sellers) used to interact with each other directly to create a complex web of connections among themselves as shown in Figure 2.

Figure 2: Central counterparties reduce complexity of trade

5. Trade repositories

A trade repository maintains a central database of transactions and data. It is a new component of FMI and is gaining importance in the OTC derivatives market. By centralizing the transactions and dissemination and storage of collected data, it enhances the transparency of information to relevant authorities and the public. An important function performed by trade repositories is to provide information that supports risk reduction, operational efficiency, and cost savings for the participating entities and the market. Trade repositories store commodities, energy, equities, interest rate and credit. Since several stakeholders use the data stored by trade repositories, it is critical to maintain accuracy, reliability, and data availability.

Security issues in central counterparties

Besides financial risks, central counterparties are prone to cyber-attacks. According to the Allianz Risk Barometer, Cyber perils are the biggest concern for companies globally in 2022, and in total, 2021 saw 50 per cent more cyber-attacks per week on corporate networks than in 2020. Juniper Research and the World Economic Forum estimated the impact of a single global cyber-attack around USD $121 billion. Beyond the financial crisis, cyber-attacks can disrupt services, financial markets, and a broad spectrum of loss of confidence. As reported by Carnegie Endowment for international peace, data breach, malware, and distributed denial of service (DDoS) are the most common cyber-attacks that resulted in significant financial losses for various financial institutions. Nonetheless, the list of individual security risks is never-ending.

Cyber-attacks are becoming more sophisticated with time. The motive of perpetrators is to induce financial instability, destabilize jurisdictions, steal data, demand money, disrupt network communications, and harass financial institutions. Evidently, payment systems, including banks, stock exchanges, and other financial firms, are the primary targets of cyber-

attacks. Based on the types of cyber-attacks witnessed by central counterparties, the following cybersecurity issues impact the financial transactions.

- **Failure of central node:** Since central counterparties are placed in the central part of the financial network, they themselves become crucial. The situation deteriorates when the central counterparties fail as clearinghouse. Considering that central counterparties manage thousands of counterparties, its failure can be a contagion. In the worst-case scenario, the financial markets may need to be shut down temporarily to resolve the situation.
- **Shock amplification through central counterparties:** Failure of central counterparties can propagate financial stress among other counterparties connected to it. The impact of shock propagation can be limited by using risk management policies for the financial system.
- **Central clearing:** To manage risks, central counterparties need to impose strict regulations on their counterparties. This includes creditworthiness, liquidity, and operational reliability of counterparties. This makes it essential to clear trade among counterparties who fall under the restrictions for adequate technical and financial resources.
- **Counterparty risk:** The risk occurs when a buyer is not able to pay the price, or a seller is unable to deliver the securities. In other words, insufficient funds are one of the reasons that cause counterparty risk. It is treated as liquidity risk.
- **Custody and investment risks:** Custody risks are associated with safekeeping securities. It consists of inadequate record-keeping, negligence, fraud, cyber-attacks, and loss of assets held by the custodian.
- **Legal risks:** Central counterparties interact with different counterparties that may belong to different jurisdictions and law bodies. This introduces legal risks to cross-border settlements.

What's next

This article introduces financial market infrastructures and its various components. It puts forward various security issues faced by central counterparties. The last article of the *Understanding cybersecurity management for FinTech* series explores cybersecurity policy and strategy management in FinTech.

WOULD YOU RECOMMEND THIS ARTICLE?

+3 0

Previous article

Why software-defined AV-over-IP modernizes enterprise communications

Next article

5 cybersecurity concerns in digital marketing

Gurdip Kaur and Arash Habibi Lashkari

***Dr. Gurdip Kaur is a Risk Advisory Consultant at Deloitte Canada. She is a CompTIA certified CyberSecurity Analyst (CySA+) experienced in detecting and analyzing malicious network traffic. She is the author of the book titled "Understanding Cybersecurity Management in FinTech" published by Springer in 2021. She has also contributed to the "Understanding Android Malware Families (UAMF)" series to the IT World Canada this year. She has published several book chapters and research papers with reputed journals. She has contributed to three public cybersecurity datasets generated at the Canadian Institute for Cybersecurity, University of New Brunswick. She was awarded two gold medals in Bachelor of Technology and a silver medal for the research project on high interaction honeypots. Her research project on malware reverse engineering was selected among top 10 projects in the National Student Project Contest in 2015. She is strongly inclined towards cybersecurity, malware analysis, vulnerability management, incident reporting, and SIEM solutions.

***Dr. Arash Habibi Lashkari is an Associate Professor in Cybersecurity at York University and a senior member of the IEEE. Prior to this, he was an Associate Professor at the Faculty of Computer Science, University of New Brunswick (UNB), and research coordinator of the Canadian Institute for Cybersecurity (CIC). He has over 23 years of academic and industry experience. He has received 15 awards at international computer security competitions - including three gold awards - and was recognized as one of Canada's Top 150 Researchers for 2017. He also is the author of ten published books and more than 100 academic articles on a variety of cybersecurity-related topics. In 2020, he was recognized with the prestigious Teaching Innovation Award for his personally-created teaching methodology, the Think-Que-Cussion Method. He is the author of 12 published books and more than 100 academic papers on various cybersecurity-related topics. He is the founder of the Understanding Cybersecurity Series (UCS), an ongoing research and development project culminating with a varied collection of online articles and blogs, published books, open-source packages, and datasets tailored for researchers and readers at all levels. His first two books in this series are entitled "Understanding Cybersecurity Management in FinTech - Challenges, Strategies, and Trends" and "Understanding Cybersecurity Law and Digital Privacy - A Common Law Perspective," published by Springer in 2021. The first online blog series of UCS entitled "Understanding Canadian Cybersecurity Laws", was recognized with a Gold Medal at the 2020 Canadian Online Publishing Awards (COPA). His research focuses

on cyber threat modeling and detection, malware analysis, big data security, internet traffic analysis, and cybersecurity dataset generation.

POPULAR BLOGS

Today's podcast reports on Toyota and global insurance broker Aon dealing with cyber attacks, updates on attacks on Axis and Nvidia attacks, and more #cybersecurity #cybersecuritytoday https://t.co/hDs7ct1GEK

7 hr. ago 1

4 hr. ago 2

.@Huawei Canada has opened the first of 15 experience stores planned across Canada in collaboration with @CC_Deals. https://t.co/xs7PNL8ecJ #Device #Retail https://t.co/QMXsmTzrhE

Last chance to nominate for the @CDN_Channel 's Channel Innovation Awards. Don't miss this opportunity and submit your nomination before March 4. https://t.co/mVdBivTTSs #CDN #Channel #CDNAwards https:

LOAD MORE POSTS

1 day ago

POPULAR STORIES THIS WEEK

Privacy & Security

Successful phishing attacks were up in 2021: Report

IT Workplace

Hashtag Trending Mar. 2 – Reddit quarantines r/Russia; Nvidia experiences cyberattack; Italy's semiconductor investment

Privacy & Security

Manufacturing was most attacked sector in Canada in 2021: IBM

Cloud

Coffee Briefing March 1, 2022 – AWS-NHL partnership; Gen Z and identity theft; Calibre Scientific opens online lab in North America; OpenText CE 22.1; and...

IT Workplace

Hashtag Trending Feb. 25 – Privacy policy hurts Meta's business; labor organizer arrested; Twitter accidentally suspends journalist account

ITWorldcanada.com is the leading Canadian online resource for IT professionals working in medium to large enterprises. IT World Canada creates daily news content, produces a daily newsletter and features IT professionals who blog on topics of industry interest.

FOLLOW US