Understanding cybersecurity management for FinTech: cybersecurity vulnerabilities and risk in FinTech (Article 4) - IT World Canada

December 1, 2021

FinTech revolves around technologies such as cloud, blockchain, AI, and mobile devices that are used for financial transaction payments, cryptocurrencies, money transfers, trading, and regulatory compliance. With so much monetary value associated with all these technologies, perpetrators are always lured to breach security by exploiting vulnerabilities that exist in these technologies, and posing risks to FinTech.

Security threats disrupt business and hence, financial stability. The attractiveness of financial gain and access to confidential data are the two most important reasons for making the financial sector one of the biggest targets. Therefore, identifying cyber vulnerabilities and risks is vital to every financial organization.

This article investigates cybersecurity vulnerabilities and risks in FinTech. It brings forward some common cybersecurity vulnerabilities

that were exploited in the past. It presents some general policies to mitigate cyber vulnerabilities in FinTech. Cyber risks induce different uncertainties in FinTech which are addressed towards the end of the article. 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

A vulnerability is defined as a weakness which can be exploited by a cyber-attack launched by a threat actor. In other words, vulnerability is a flaw, loophole, error, limitation, oversight, or susceptibility in any aspect of FinTech, especially the IT environment. If vulnerability is exploited, it can cause severe losses or damage to the assets. These losses or damages are referred to as risks.

National Institute of Standards and Technology Special Publication (NIST SP) 800-28 Version 2 defines cyber risk as *"A measure of the likelihood and the consequence of events or acts that could cause a system compromise, including the unauthorized disclosure, destruction, removal, modification, or interruption of system assets".*

Figure 1 highlights the timeline of cyber risk trends in the global economy. Apparently, cyber risk began to trend in the third quarter of 2014 and then declined till the first quarter of 2016. It remained stable in 2016 and started to increase gradually until the third quarter of 2017. With a consistent value in 2018, it has been decreasing since 2019.

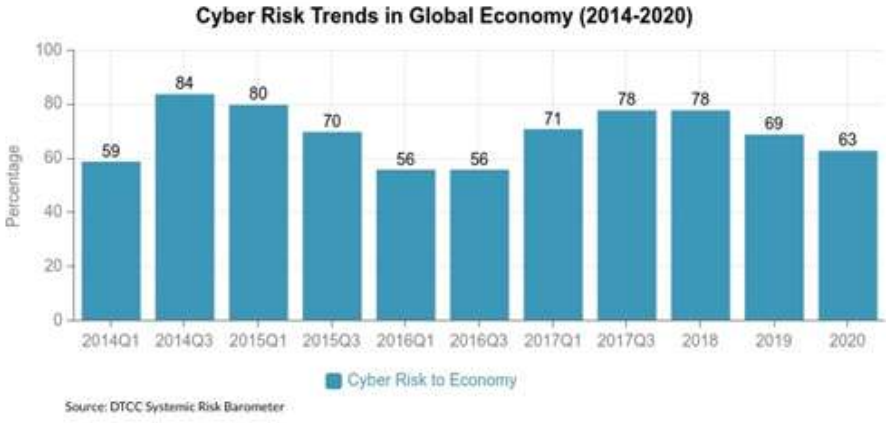

Figure 1: Cyber risk trends in the global economy (2014-2020)

Common cyber vulnerabilities in FinTech

Despite the fact that innovative technologies have contributed to the evolution of FinTech, these technologies also bring the fear of exposing several vulnerabilities that can be exploited at no extra cost. Some of the general vulnerabilities in the technologies, platforms, frameworks, and related solutions used by FinTech are summarized below.

- **Money laundering:** Most of the financial institutions are vulnerable to money laundering. The term is used to refer to making substantial amounts of money through illegal activities and processing it to make it clean and come from a legitimate source.
- **Phone verification without OTP:** This vulnerability bypasses the authentication process of confirming a One-Time Password (OTP) generated as a part of the financial transaction.
- **Ransomware:** It is a type of malware that encrypts files and directories on the target computer to disrupt authorized access and demand a handsome amount of ransom to provide the decryption key.
- **Information disclosure:** It is a vulnerability in which sensitive information is revealed intentionally or unintentionally to unauthorized personnel.
- **Unpatched operating system and applications:** Unpatched operating systems and applications expose vulnerabilities to attackers who are always peeping into the security flaws. Security breaches due to exploitation of vulnerabilities exposed by unpatched software can run rampant on business owners by reducing productivity and economic stability.
- **Injecting malware to steal login credentials and other important data:** Use of smartphones for online banking and payment is an essential application of FinTech. Attackers inject malicious code into mobile applications to steal login credentials and use them to perform financial fraud, especially credit card fraud.

- **Auto saving login credentials:** Some users prefer to save their login credentials rather than remembering them. The web browser stores the session cookies and the username and password used to log in to the system. If an attacker hijacks the session, he can easily steal login details.
- **Lack of cyber education:** There is a lack of cyber education and training among common people so that they can be made aware of what vulnerable situations are and how to respond to those situations to stay protected.
- **Non-compliance with organization policy:** Every financial institution has its own crypto-compliance policy to abide by the rules and guidelines laid out to protect against FinTech crimes such as money laundering, financial terrorism, and malicious cryptocurrency exchange.

General policies to mitigate FinTech cybersecurity vulnerabilities

Based on the types of vulnerabilities discussed above, every FinTech institution designs a policy to implement basic regulations to avoid or treat the identified vulnerabilities. These policies are based on factors influencing the budget, market value, infrastructure cost, and reputation of the institution. Some essential policies for providing fundamental security for the financial work of an institution are streamlined below.

- **Computer literacy:** Educate users to understand common cyber threats, especially phishing, eavesdropping, and social engineering tactics.
- **Social media interactions:** Users must also be aware of the extent of social media interactions which include posting professional or work-related information on personal accounts and accepting friend requests sent by strangers or acquaintances.
- **Background checks:** One of the important aspects of recruiting a new employee is to have a background check. It facilitates financial institutions to investigate a candidate's education, criminal background, and employment history.

- **Password complexity:** Password complexity rule includes choosing a password with a combination of lowercase and uppercase alphabets, numbers, and special characters.
- **Removable device usage:** Personal removable devices may inject malware into office computers and workstations. Therefore, it is a common policy to prohibit the use of removable storage media such as USB drives in office machines.
- **Clicking on hyperlinks in email:** All the employees must be educated about phishing attacks and opening links in emails received from outside the organization. External emails need to be opened carefully and employees must know that they must not click any hyperlinks in the luring emails.
- **File access logs:** Some organizations verify the file access logs to determine who has accessed sensitive files and at what time and for what duration. A logbook is maintained to record all the entries related to accessing a confidential file.

Kinds of uncertainties resulting from cyber risks

FinTech uncertainties can be broadly divided into three categories:

1. **The dominance of banks over technology:** Despite growing technologies, there are still many banks that prefer to work in the traditional way. These banks fear technological disruption. Their reluctance to emerging technology and preference for traditional working culture makes the future of FinTech uncertain.
2. **Data breach:** Information theft or data breach is one of the important challenges for FinTech. FinTech companies deal with sensitive financial data that includes credit card details and personally identifiable information. Cybercriminals steal information and sell it for monetary gain. Stolen information is also used by hacker groups to send phishing emails, emulate personal identity, illegally transfer money, money laundering, and fund nation-state terrorist activities. Surging data breaches is a cause of concern for financial institutions since it adds to the uncertainty of FinTech security.

3. **Cyber risk:** The unrivalled threat of cyber risk is creating havoc in the FinTech industry. Only a handful of cyber incidents are reported from a massive pool of total cyber incidents per year. Many financial institutions believe that concealing cyber incidents helps them not to reduce their market value. However, reality is something else. A financial institution may be attacked again if the vulnerabilities are not fixed. Implementing a cyber risk management solution is necessary to compute cyber risks in advance and plan some measures to mitigate them at the earliest.

Handling uncertainty for FinTech cybersecurity risk

Based on the types of cyber risks and uncertainties resulting from them, following measures can be adopted to reduce the impact of these uncertainties.

- **Secure digital transactions:** Digital transactions need to be governed by a secure communications protocol standard that ensures the security of credit card transactions over the Internet. One example of a secure communication protocol standard is Secure Electronic Transaction (SET). It was initially supported by Mastercard, Visa, Microsoft, Netscape, and others. It uses a digital certificate that verifies a transaction among merchants by using a combination of digital signatures and digital certificates. In this way, it enforces the privacy and confidentiality of digital data.
- **Know your vulnerabilities:** One basic principle of cybersecurity is knowing the enemies you need to fight with. For an effective FinTech cybersecurity risk management system, it is imperative to list the vulnerabilities in the system that may be exposed to internal and external threats. Once weaknesses are known, proper measures can be taken to fix them to avoid any risks.
- **Compute risks:** FinTech companies must be aware of the potential cyber risks that can impact their business. Computed risk scores help to prioritize some risks over others. This way, companies can address severe risks with appropriate remedies.

- **Backup data regularly:** One of the protective measures in the cybersecurity arsenal is to back up the data at a regular interval of time. It aids in keeping a copy of the essential data files on an alternative server. In case the primary server is under distributed denial of service attack or ransomware attack, the users can access their data from the alternative server. It also always ensures the availability of data.

What's next

This article introduces cyber vulnerabilities and risks in the FinTech industry. It puts forward common cyber vulnerabilities and risks posed by them. The mitigation measures for dealing with uncertainties are also discussed. The next article of the *Understanding cybersecurity management for FinTech* series explores security issues on the financial market infrastructures.

Would you recommend this article?

+3

0