Cyber Security challenges for FinTech’s

## A picture containing text, sky Description automatically generated

Due to unfortunate recent pandemic many of the consumers found themselves stuck at home with free time at hand. They also do not want or need to go to the bank and spend hours in lines for basic transactions.

This inevitably led to the rapid growth in demand of online shopping and use of Mobile and Web based financial services. Unfortunately, cyber-criminals have also noticed this trend and quickly adapted there activities accordingly. As per one report 625 thousand users were attacked by different kinds of banking trojans in 2020.

Incumbents have been in this business for a long time and have had a head start in developing Security Policies, Procedure, and Processes in addition to the implementation of operational, technical and management controls although not nearly enough to prevent cyber security threats.

Fintechs to compete with Incumbents and earn customer’s trust, they need to adapt and ensure security of customer’s data.

In this article we have discussed the challenges being faced by FinTech’s as they embrace the new reality of everchanging nature of cyber security threats. We also provide possible solutions in dealing with these threats.

Security threats to Web Applications

To service customers, FinTech companies often rely on web applications. These applications with distributed architectures comprise of many third-party libraries and services and are by design, available for everyone around the world. This is the reason why cyber-criminals are more inclined to directly attack web applications and use their weak and insecure code as a gateway to the company’s infrastructure and network.

Earlier in the last year, Greece’s four main banks – Alpha Bank, Piraeus Bank, Eurobank and the National Bank of Greece - were forced to cancel 15,000 credit and debit cards when cybercriminal breached the Greek tourist services portal on their web application.

Mitigation: There are multiple different strategies that need to be adapted to prevent cyber- criminals from exploiting web applications.

1. Developers must understand secure code paradigm, security vulnerabilities and follow secure coding guidelines.
2. Web application penetration testing, code review and vulnerability assessment by a reliable third-party.
3. Vulnerability Management mapping system with the capability to provide insights and generate alerts as and when new vulnerabilities are identified against the systems and software installed within an organization.
4. Network and Web based firewall and Intrusion prevention systems to detect and block cyber security threats.
5. Threat Intelligence on latest Indicators of compromise (IOC’s), information on Cyber-criminals/Groups actively involved in exploiting known and unknown vulnerabilities within the industry.
6. Security Incident and Event Management system (SIEM) to monitor, analyze and respond to security incidents.

Security Threats to Mobile Apps

FinTech services are usually served through mobile applications. Mobile banking security depends on Secure Software Development Lifecycle (SSDL). Major issues seen are code vulnerabilities, Insecure data storage, insecure data display and implementation of insecure authentication and encryption mechanisms.

If the Mobile banking App is not secure, cyber-criminals can clone, modify Mobile App obtain credentials and duplicate customer identities and send malicious code to the banking system to initiate cyber-attack to gather data and perform unauthorized transactions, in addition to the attacks generated by other malicious Mobile App’s installed.A picture containing graphical user interface

Description automatically generated

Mitigation: For a comprehensive protection it is highly recommended for Fintech’s and Banks to have a third-party perform a detailed Mobile App security assessment.

Some of the areas that threat assessment must identify are the implementation of sufficient code obfuscation, code protection from injection and repackaging, SSL pinning, secure data and key storage, emulator and overlay detection and two- factor authentication.

# Ransomware attacks

Ransomware attacks are a major threat to the FinTech services. The problem with ransomware attacks is, when it happens even major security vendors are usually unable to recover the locked data. There is no “recovery” tool that can guarantee full recovery of all infected data.

Unfortunately, as common as these attacks are most of the companies are unable to take mitigation actions against these attacks. Diebold Nixdorf, which controls around 35% of the global ATM market, owned up to a ransomware attack in May. In early April, the average price asked for by attackers was around 60 BTC, or $570,000.

A screenshot of a video game

Description automatically generated with medium confidence

Mitigation: Frequent data backups and end point protection mechanisms should be in place as part of defense in depth strategy to mitigate such attacks.

# Insider attacks

Having more detailed knowledge of working of company’s network, insider threats pose a grave danger to the company.

Postbank, the banking division of South Africa’s Post Office, had to replace more than 12 million of its customers’ cards after a group of its employees printed and then stole its master key. Rogue employees accessed user accounts between March and December 2019 to make more than 25,000 fraudulent transactions.

Mitigation: Security policy enforcement, implementation of least privilege access, segregation of duties and security monitoring plays a key role in mitigating insider attacks.

# Customer Data Theft and Dark web Leaks

As FinTech deals with personal data of its customers, they are concerned about theft of such data and leaking them or threat to release it on Dark web.

On Mar 24, 2021 Pligence Threat Intel Focus group reported on social media about a threat actor that dumped 400k+ data of a Pakistani Bank named FCI Bank on a popular hack forum. The Dump allegedly contained Email Addresses, Usernames, Passwords, and other Personally Identifiable Information (PII).



Mitigation: Threat Intelligence system to identify data leaks in a timely manner to prevent unauthorized financial transactions, report leak to the relevant authorities and customers to prevent further damage in addition to Identification of Cyber-criminals/Groups, tools, techniques, and procedure (TTP’s) used in the attack to prevent any further cyber security attacks.

# Phishing attacks

Phishing attacks are conducted by cyber-criminals when they send you an email with malware as attachment or divert you to the legitimate look alike website which installs malware or they contact you in person impersonating as someone to ask for credentials or other private information, later known as social engineering.

Black hat hackers regularly take advantage of human error and access applications and user accounts by conducting phishing and spear attacks. But unfortunately, companies are unable to defend their infrastructure against these attacks. The Financial Conduct Authority (FCA) admitted to a data breach after victims of the collapsed savings firm London Capital & Finance (LCF) were sent messages by scammers. LCF customers’ names, addresses and phone numbers were accidentally published on the FCA’s website. The details were gathered by the FCA during a complaint’s procedure against LCF.

Graphical user interface, application

Description automatically generated

Mitigation: Phishing and Spear phishing attacks can be mitigated by Staff training, situational awareness training and implementation of Sandboxes, Proxy Servers and Threat Intelligence systems to identify malware, malicious website URL’s, Indicators of compromise and latest techniques being employed within the industry.

FinTech services’ integration with legacy bank infrastructure

Many of FinTech customers deal with traditional banks. Most of them move their funds to and from traditional bank accounts to use FinTech services.

The problem is most of these cutting-edge FinTech services rarely integrate with banks large and legacy systems. To make them work custom-built integration which are known as Application Programming Interfaces (APIs) are implemented which ensures that all systems, old and new, can communicate with each other. However, these APIs may take months to develop and security, being a quality attribute, require extra time and resources to achieve.

A company may cut cost due to economic downturn or provide less time to securely develop APIs which will cause the service to be more likely to exposed to cyber vulnerabilities.

Mitigation: Focusing on Security during Software Development Life Cycle (SDLC) and ensuring all software passes certain security standards by implementing security related test cases.

In case of outsourcing the development, choosing a third-party security focused testing team can also help in delivering a safe and secure product.

Third-party risks

In addition to their own developed products, Fintech service provider also use third-party software. These software have their own vulnerabilities and weaknesses that cybercriminals can use to hack into. This third-party software may also not have developed security in mind. This can make them riddled with security flaws. Hackers can implement an attack known as supply chain attack in which they compromise third-party to get access to the data.

Mitigation: Third-party risks can be mitigated by conducting regular security audits. Deployment of vulnerability management mapping system for a better insight into the vulnerabilities and information on deployed systems and software within the organization.

Data privacy

As FinTech Industry deals with user’s personal data, hence it becomes vital for them to properly protect this data from illegitimate access.

FinTech service providers must store and transmit the data in a secure way to protect their customers. Failure to do so can lead to data leak and/or heavy fine from governments.

In April 2019, Facebook faced a lawsuit of worth $2.2 billion for storing passwords in plain text by mistake.

Mitigation: Comply with local governments’ privacy laws and international standards such as GDPR, ISO, etc. Transmission and storage customer’s Personnel Identified Information (PII) and financial data should be done using strong encryption protocols, access to data should be secured by implementing a multi-factor authentication and authorization mechanisms. Last but not least vigorous monitoring and analysis of security event and Incidents.

# Final Thoughts

Fintech’s have a key role to play in the financial services industry as they continue to develop and grow in this fast-paced environment. Therefore, to acquire new customers and win their trust, Fintechs need to have comprehensive Cyber Security management, operational and technical controls in place to prevent cyber security attacks and cyber-criminal from stealing customer information and financial data.