FEATURE

Cybersecurity and Fintech at a Crossroads

Financial technology (fintech) is a prominent topic for the banking and financial services industry worldwide. Although its disruptive and innovative technologies provide banking services to populations who never before had access and easier investment and loan processing for others, enterprises implementing fintech need to address the new risk factors that are associated with this solution.

What Is Fintech?

Fintech refers to disruptive technologies that enable the development of innovative financial systems and the delivery of financial services in a more efficient manner to add greater value to customers. Economic globalization developments have resulted in increasing needs for financial services that are diverse and complex. Fintech brings innovations to consumer services and banking and financial back-end services by addressing this diversity and complexity and bringing a wide range of benefits to the economy. Global banks and financial services enterprises can leverage fintech to improve efficiency, lower operating costs, and offer a wider range of products and services.

Fintech Brings Cybersecurity Risk

Enterprises that implement fintech face cybersecurity risk from integration issues such as compatibility and legacy technologies. Integration of fintech with traditional banking systems may raise concerns regarding data privacy. Fintech enterprises collect large volumes of customer data, including sensitive personal information, making them ripe targets for hackers.

Fintech brings easy access to core banking activities to people who could not access these services previously. These new bank customers have little or no previous awareness of cybersecurity risk and, therefore, may be more exposed to hackers.

Fintech offers easily accessible services through application programming interfaces (APIs) exclusively developed for banks to access the fintech platforms, which is called API banking. The use of open APIs enables third-party developers to build applications and services around the needs of banks, which is called open banking.

The complexities and technical dependencies that exist between various technologies integrated in a fintech ecosystem have made it a very ripe target for hackers. Fintech implementation interfaces with banks, financial service providers and fintech firms, which increases cybersecurity risk as data elements travel through these interfaces.

Third-Party Security Risk

When banks establish formal relationships with fintech service providers to leverage their services, banks take on third-party security risk such as data leakage, service failures, litigation and reputational damage. Banks should consider the fintech-relationship-related risk in their third-party risk management assessment.[1]

To mitigate third-party security risk factors, organizations should consider implementing the following proactive measures:

- Third-party security policies

Vimal Mani, CISA, CISM, Six Sigma Black Belt
Is the head of information and cybersecurity operations of Bank of Sharjah. He is responsible for bank information and cybersecurity programs, coordinating security operations across the bank branches in the Middle East. Mani is also responsible for coordinating bankwide security strategy and standards, leading periodic security risk assessment efforts, incidents investigation and resolution, and coordinating security awareness and training programs. He is an active member of the ISACA® Dubai (United Arab Emirates) Chapter. He can be reached at vimal.consultant@gmail.com.

© 2019 ISACA. All rights reserved. *www.isaca.org*

- Nondisclosure agreements and confidentiality agreements
- Periodic security risk assessments of third parties

To effectively address third-party risk, organizations need to work with all those parties providing various services/products to them on an ongoing basis to ensure that any current and future risk within the services/products that they supply are identified in a timely manner and appropriate risk prevention/mitigation measures are taken.

Malware Attacks

Hackers targeting the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system are getting more sophisticated. The SWIFT system is used by banks and financial services organizations worldwide to securely transfer information about financial transactions. The sophistication level of malware is demonstrated by recent cyberattacks on the SWIFT/automated teller machine (ATM) infrastructure of the second-largest bank in India.[2] A recent report illustrates that easily exploitable vulnerabilities are prevalent in banks, and hackers take advantage of these vulnerabilities by launching malware attacks.[3]

To address malware risk, organizations should consider implementing the following proactive measures:

- Endpoint security solutions
- Endpoint protection and prevention (EPP) solutions
- Endpoint detection and response (EDR) solutions
- Sandbox-driven email gateway servers
- Distributed denial of service (DDoS) prevention solutions
- Ongoing security awareness and trainings on malware attacks

To effectively address the emerging innovative cyberattacks, the interaction of various new-age malware prevention technologies including host and network-based IDS, EPP and other emerging new technologies such as EDR is needed. Combining various malware prevention technologies provides robust coverage against the dynamic and innovative malware attacks emerging in the industry these days.

Data Leakages

Financial data such as payment card information and user credentials are vulnerable to data-leakage attacks when banks venture into fintech partnerships with third-party fintech firms. Automated systems that interface with fintech service providers are particularly vulnerable to sensitive financial data leaks.

To address the data leakage risk, organizations should consider implementing the following proactive measures:

- Data classification for all the critical information assets
- Data leakage/loss prevention (DLP) solutions
- Disabling Universal Serial Bus (USB) and CD drives in laptops and desktops

Data loss is a common and perennial problem faced by global organizations that has no single silver bullet solution. Organizations should consider leveraging various best practices around DLP implementing best of breed DLP solutions that will better fit the needs of organizations. Also, organizations should focus on identifying all the potential data loss modes and prioritizing them based on past breaches, the likelihood of breaches and the number of potential users having access to those data loss modes.

Data Integrity Risk

Mobile devices play a predominant role in fintech banking services. If mobile devices without strong encryption algorithms are used for fintech services, integrity issues regarding the financial data that are communicated over the cluster of fintech interfaces may result. Researchers found that the integrity of data that are gathered from fintech applications such as mobile money applications varied dramatically across their samples.[4]

To address the data integrity risk, organizations should consider implementing the following proactive measures:

© 2019 ISACA. All rights reserved. *www.isaca.org*

- A robust input validation controls
- Solutions preventing entry of erroneous inputs
- Provision of access rights strictly on a need-to-know basis
- Robust backups

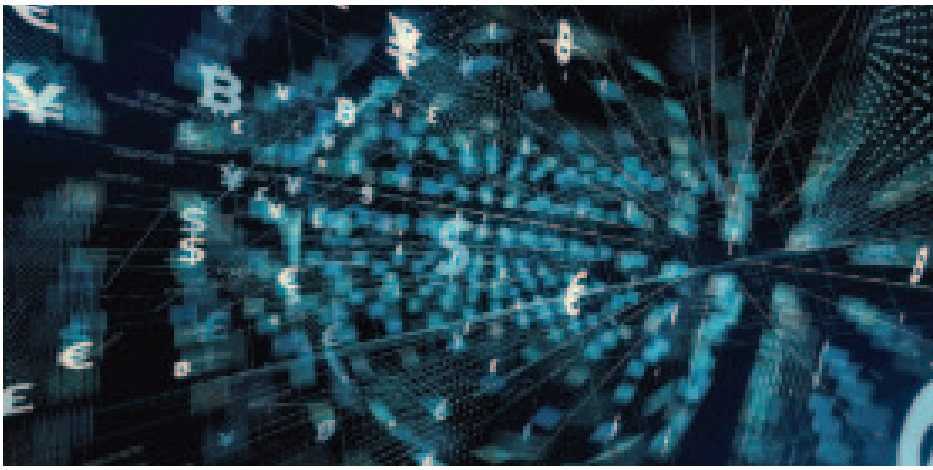
Implementing data management tools, robust backup and recovery systems, making copies of all the data, robust storage media management, and effective management of storage devices such as SAN, NAS and DAS will help organizations address data integrity issues. Maintaining audit trails helps organizations track data integrity issues in an effective manner. To address data security and integrity problems in software development, organizations have started using methodologies such as DevSecOps and the Open Web Application Security Project (OWASP) standards. DevSecOps is a recent development methodology that emphasizes people and processes and seeks to improve the level of collaboration between development, security and IT operations teams.

Cloud Environment Security Risk

Cloud computing is one of the major enablers of a fintech ecosystem. Payment gateways, digital wallets and secure online payments are some of the niche cloud computing services provided in a fintech ecosystem. For example, making payments is very easy and fast through cloud computing. Maintaining the confidentiality and security of financial information is critical to banks and financial services. Lack of adequate cloud security measures can result in compromise and corruption of this sensitive information. This risk can be avoided with a strong encryption mechanism for the cloud platform.

To address the cloud-environment-related security risk, organizations should consider implementing the following proactive measures:

- Risk assessment of the cloud service provider before establishing the relationship
- Robust encryption technologies
- DLP solutions
- DDoS prevention solutions



- API security solutions
- Single sign on (SSO) solutions

Assessing the security posture of cloud service providers (CSPs) is essential in ensuring security of information maintained by them. Encryption and digital signatures should be considered as the critical confidentiality and integrity protection mechanisms for information maintained in public cloud environments. Legacy applications may need analysis and enhancement before deploying them in cloud environments. Data replication provided to CSPs should not be considered as the only option for backing up the information maintained in a cloud environment. Also, privacy assurance responsibilities should be reviewed if organizations consider moving personally identifiable information (PII) to a cloud environment.

> “AUTOMATED SYSTEMS THAT INTERFACE WITH FINTECH SERVICE PROVIDERS ARE PARTICULARLY VULNERABLE TO SENSITIVE FINANCIAL DATA LEAKS.”

Application Security Risk

Fintech implementation is driven by various banking systems that need to access financial profiles of banking customers to perform real-time transactions. Applications are always preferable

© 2019 ISACA. All rights reserved. *www.isaca.org*

“IT LEADERS WHO ARE PLANNING TO IMPLEMENT FINTECH NEED TO ENSURE THAT FOOLPROOF APPLICATION SECURITY MEASURES ARE IMPLEMENTED TO PROTECT THE CUSTOMER DATA THAT RESIDE IN THE VARIOUS BANKING SYSTEMS THAT WILL GET CONNECTED WITH A FINTECH PLATFORM.”

attack vectors due to the vulnerabilities that are hidden in their design and code. IT leaders who are planning to implement fintech need to ensure that foolproof application security measures are implemented to protect the customer data that reside in the various banking systems that will get connected with a fintech platform. Design that is driven by OWASP guidelines, code reviews and penetration testing needs to be performed during fintech integration.

To address the application security risk, organizations should consider implementing the following proactive measures:

- Periodic vulnerability analysis
- Vendor recommended patches in timely manner
- Conducting application security risk assessments in periodic intervals
- OWASP guidelines for application development
- DevSecOps standards for application development
- Web application firewalls (WAF)
- SSL proxies
- Multifactor authentication (MFA) solutions

Implementing techniques such as Static Application Security Testing (SAST), Source Code Analysis (SCA), Dynamic Application Security Testing (DAST), penetration testing, Runtime Analysis, Automated Regression Testing and adopting DevSecOps methodologies in application development helps organizations address application security risk effectively. Adopting DevSecOps helps organizations identify and address application security vulnerabilities throughout the continuous integration and continuous deployment environments. As more organizations globally have started adopting Agile methodologies for realizing faster application deployments, incorporating DevSecOps into their development environments helps them in identifying security risk factors within applications at a faster pace.

Digital Identity Risk

Introduction of technology-driven banking using mobile devices with one-time passwords (OTPs) and security codes creates the risk of digital identities of banking customers being misused. Most fintech applications are web applications or services where mobile devices work as front end. So banks and financial services organizations need to revisit their electronic banking security architecture to address these risk factors before planning for fintech implementation.

To address digital identity-related risk, organizations should consider implementing the following proactive measures:

- Implementation of robust digital identity-proofing methods
- Implementation of identity fraud prevention solutions
- Implementation of best practices such as the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 Digital Identity Guidelines

Analysis of identity theft incidents is critical for understanding the nature of identity theft and identifying effective solutions for preventing such theft from happening in the future. Increasing the awareness of identity thefts better enables organizations to develop management strategies and robust identity governance for preventing identity theft. Also, organizations should consider implementing comprehensive identity management solutions fit for different application domains.

© 2019 ISACA. All rights reserved. *www.isaca.org*

Legacy Banking Systems Are Risk Factors for Fintech Implementation

Globally, banks are struggling to develop and implement new technologies rapidly in response to their underperforming and outdated, non-patched core banking systems, which are vulnerable to various kinds of cyberattacks. While fintech integration will happen with such legacy systems, the fintech platforms will also become preferable targets for hackers. Banks aspiring to get into fintech need to prioritize refreshing their core banking systems.

Money Laundering Risk

Unlike traditional banking systems, fintech-driven banks are more likely to be used for money laundering activities because fintech often uses cryptocurrency for financial transactions. Cryptocurrencies are one of the integral elements of a fintech ecosystem that is not formally regulated based on any global standards and regulations. Use of nonregulated cryptocurrencies can result in illegal money laundering and terrorism funding. Identifying the beneficiary in any fintech-enabled transactions is not possible due to fintech's pseudonymous nature, which can be a significant support to money laundering operations.

Technology Risk

Apart from the risk discussed herein, there is other potential technology risk for an enterprise that is starting a fintech venture. To address the technology risk, it is recommended to follow the Monetary Authority of Singapore "Technology Risk Management Guidelines"[5] and the Reserve Bank of India "Cyber Security Framework in Banks" guidelines.[6] Apart from these two sets of guidelines, there are many other cybersecurity guidelines made available to banks by various regulators. But, due to their comprehensive coverage and relevance to financial services sector, these two guidelines are especially useful.

The use of IT by banks has grown rapidly, which has become very critical from a business point of view. The Reserve Bank of India (RBI) had provided guidelines on information security, electronic banking, technology risk management and cyberfraud. Banks need to proactively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging cyberattacks.[7]

The Monetary Authority of Singapore (MAS) has issued the Technology Risk Management (TRM) guidelines, which addresses existing and emerging technology risk within financial institutions.[8] The MAS TRM guidelines help banks identify security and risk management issues in a comprehensive manner, covering everything from identity assurance and access controls to accountability and audit.

> "BANKS ASPIRING TO GET INTO FINTECH NEED TO PRIORITIZE REFRESHING THEIR CORE BANKING SYSTEMS."

Blockchain Risk

Blockchain platforms are used as part of the fintech ecosystem of many enterprises. Although blockchain is very efficient and quickly executes transactions, the following significant concerns about the security of blockchain-based transactions in a fintech ecosystem can cause risk to the ecosystem:

- Blockchain can be hacked like any other platform/protocol. If someone chooses to save their bitcoin and private keys on an Internet-connected device, they can be stolen. After private keys are stolen, secure blockchain architecture and encryption features are of no concern to hackers.
- Blockchain can be infected by malware. Researchers have demonstrated that botnets have the ability to send messages utilizing the bitcoin network. The Fujacks trojan, a botnet backdoor, has successfully proven that it can

© 2019 ISACA. All rights reserved. *www.isaca.org*

remotely control infected computers that are nodes in a blockchain, collect information, and install other malware or tools into the blockchain.[9]

- Banks have concerns about transaction confidentiality, securing private keys and the strength of cryptographic algorithms that are used in blockchain-based transactions.
- Any blockchain transaction is dependent on trust between two or more parties. Most people use bitcoins at exchanges and trust that the exchange will look after them. Many money exchange firms are not fully regulated entities. They cannot offer assurance on the transfer of digital currencies.

> "USE MACHINE LEARNING EFFECTIVELY TO IMPROVE THE CYBERSECURITY POSTURE OF THE FINTECH VENTURE."

Addressing Fintech-Triggered Cybersecurity Risk

The following are recommendations to protect an enterprise from the potential risk of implementing fintech:[10]

- Avoid using public clouds, which are vulnerable to data leakage risk.
- Refresh the legacy IT infrastructure and core banking systems.
- Use machine learning effectively to improve the cybersecurity posture of the fintech venture.
- Implement digital identity protection solutions.
- Institutionalize well-defined third-party security measures.
- Scrutinize the procurement of new technology solutions from a security point of view.
- Strengthen access control mechanisms.
- Implement well-defined data privacy rules.
- Consider implementation of Security Orchestration and Automated Response (SOAR), Security Operations and Analytics Platform Architecture (SOAPA), and User and Entity Behavior Analytics (UEBA) security orchestration solutions, which help in proactive incident response.
- Refer updated threat intelligence through threat feeds and automated endpoint detection response (EDR)/managed detection and response (MDR) solutions.

Conclusion

The increasing number of interfaces in fintech implementation will continue to increase the opportunities for cybersecurity risk. If hackers are successful in their efforts to compromise the fintech platform, the confidence of banking customers in the technology-driven fintech platform banking model may be reduced, which will slow the growth of the fintech industry. By implementing robust and effective cybersecurity risk management controls, enterprises can protect their fintech-driven banking system from emerging cyberattacks.

Endnotes

1 University of Southern California Gould School of Law, "OCC Guidelines for Banks Working With Third-Party Fintech Companies," 2018, *https://onlinellm.usc.edu/blog/occ-guidelines-for-banks-working-with-third-party-fintech-companies/*

2 Kolesnikov, O.; "Securonix Threat Research: Cosmos Bank SWIFT/ATM US $13.5 Million Cyber Attack Detection Using Security Analytics," Securonix, 2 October 2018, *https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/*

3 Positive Technologies, *How Hackers Rob Banks*, 21 May 2018, *https://www.ptsecurity.com/ww-en/analytics/banks-attacks-2018/*

© 2019 ISACA. All rights reserved. *www.isaca.org*

4 Anton-Diaz, P.; "New Data Security Study of Fintech Apps Highlights Vulnerabilities," Center for Financial Inclusion, 5 September 2018, *https://www.centerforfinancialinclusion.org/new-data-security-study-of-fintech-apps-highlights-vulnerabilities*
5 Monetary Authority of Singapore, "Technology Risk Management Guidelines," June 2013, *http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf*
6 Ravikumar, R.; "Cyber Security Framework in Banks," Reserve Bank of India, 2 June 2016, *https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0*
7 Reserve Bank of India, "Cyber Security Framework in Banks," 2 June 2016, *https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0*
8 Monetary Authority of Singapore, "Technology Risk," *http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/technology-risk.aspx*
9 Samani, R.; C. Beek; "Blockchain Transactions Create Risks for Financial Services," McAfee, 16 December 2015, *https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/blockchain-transactions-create-risks-financial-services/*
10 Mani, V.; "A View of Blockchain Technology From the Information Security Radar," *ISACA® Journal,* vol. 4, 2017, *http://www.isaca.org/Journal/archives/*

© 2019 ISACA. All rights reserved. *www.isaca.org*