Telecom Business Review
16 (1) 2023, 27-34
http://publishingindia.com/tbr/

Importance of Cybersecurity and RegTech in FinTech

Ajay Bansod*, Arocia Venice**

*Information Security Manager, Synclature. Email: ajayaj1995@gmail.com

**Associate Professor, DMI-st. Eugene University, Lusaka, Zambia.
Email: director_ivdl@dmiseu.edu.zm

***Abstract*—**The digital infrastructure of FinTech and RegTech, applications have been at the threat of attackers ever since the development of technology-based methods used for transactions and other banking purposes. Many banks have preyed on cyber-attacks such as ransomware, malware, Denial of Services, etc. Digitalization has provided comfort to consumers, but it has its trade-offs. Data innovation is presently seen as a potential development for stirring up the conventional Banking industry. FinTech and RegTech have been a big boon in terms of advancement in digitalization. However, the new episodes at the macroeconomic level like the 2008 monetary emergency or, significantly more recently, the Snowden case, the administrative climate is going through extreme changes. Due to this, banks and any other financial institutions' cyber risks can cause catastrophic damage to the economy. Hence the purpose of this paper is to comprehend the threats encountered by the FinTech world and explore the vulnerabilities that can lead to substantial financial losses, the ways to mitigate the danger of any cyber-attack using cybersecurity and RegTech, and ultimately avoid any economic calamity.

***Keywords*—**Cybersecurity, FinTech, RegTech, Digitization, Financial Institution, Compliance

I. INTRODUCTION

FinTechs, often known as financial technology businesses, are typically fast-growing, tiny start-ups that offer part of their products to the banking sector. Because they aren't banks, fintech companies are less closely regulated and have more latitude in responding to market demands. As a result, a fintech business can work as a bank's "overlay," making it easier to provide some financial products. Fintech is one of the fastest-growing sectors with several start-ups, e-commerce, and technology companies operating in this space across the globe. Fintech has disrupted financial business and has posed challenges for traditional banks, financial institutions, central banks, and regulatory bodies (Pant, 2020). Banks frequently use fintech because of the added benefit they provide to the banking sector—shorter time to market for services. However, this overlay often has lax security precautions (Schueffel, 2016).

RegTech is a technology that is starting to catch on across the financial services industry. It makes use of cutting-edge technologies like blockchain, AI, machine learning, and natural language processing to significantly improve how well businesses can navigate the complex regulatory environment (Arner, Zetzsche, Buckley & Barberis, 2017).

RegTech can analyze massive amounts of legal language and automatically spot places where additional compliance would be necessary for a reworked, efficient procedure.

The fact that it is a relatively new key to unlocking the door to better operational compliance does not mean, however, that it should be the sole factor taken into account by businesses wanting to improve their overall operational hygiene and security posture. Ensuring compliance alone is insufficient. Companies must also take the initiative to rectify their weaknesses, and in this case, improved cybersecurity is essential.

Cybersecurity helps protect systems connected to the internet from different threats in cyberspace. It assists in protecting software and data to prevent malware and cybercriminals from accessing other devices or networks. Cybersecurity keeps data, equipment, and information safe and secure. People use the internet to store vast amounts of data and information on numerous gadgets and other devices. Passwords and bank information are just two examples of highly sensitive information. If cybercriminals gain access to this information, it

could result in many issues, including loss of personal information and other sensitive data. Possessing sensitive information, bank OTPs, different passwords, etc., by hackers can lead to financial losses. Moreover, the hacker can alter an individual's data and use it for blackmail purposes.

Many companies need a cybersecurity structure to store their critical and confidential information. Cybersecurity helps in securing finance data and other intellectual property of the company. In government or public services, cybersecurity helps to ensure the community of securing companies' data (Lee & Shin, 2017).

Legal requirements force banks to provide dependable and secure services and create strong cybersecurity policies and operational processes to maximize those services. This is how cybersecurity in banking is enforced. Because they don't want to risk reputational damage or financial penalties, prominent and wealthy businesses frequently test their security measures. Even a modest security breach can drive thousands of customers away from huge international banks, a risk that no company should take. Above necessary, breaking the law frequently results in harsh financial penalties; these costs might harm more than a loss of clients (Najaf, Mostafiz & Najaf, 2021).

A. Benefits of Cybersecurity

- Unauthorized access to networks and data can be prevented with the help of cybersecurity.
- Assist in increasing stakeholder trust in the company's security arrangements.
- Enhance a company's credentials by implementing the appropriate security controls in various areas.
- The most crucial thing is to make fast recovery times in the different events of a breach.
- Look for and quickly recognize dangers in chronicled logs.

B. Benefits of Cybersecurity

The paper's objective is to understand the threats encountered by the FinTech world and explore the vulnerabilities that can lead to substantial financial losses, the ways to mitigate the danger of any cyber-attack using cybersecurity and RegTech, and ultimately avoid any economic calamity. The compliance challenges the FinTech companies face with ever-evolving regulations put more emphasis on the fact that FinTech, RegTech, and Cybersecurity go hand in hand. This research paper tries to address the following research questions:

- How FinTech companies will manage additional regulations for compliance?
- How to maintain compliance and uphold risk management within the growing FinTech sector?
- What are the threats and vulnerabilities encountered in the FinTech world?
- What are the ways to mitigate the threats?

II. LITERATURE REVIEW

Since the financial crisis of 2008, which affected markets in Europe and Asia in addition to the United investment in FinTech has increased quickly. To stay competitive in the market and satisfy consumer demand for products and services, financial institutions work to reinvent or create new products and services. The technological improvements within financial institutions narrowed the scope and made it necessary to develop within the regulatory and compliance spectrum. Technology breakthroughs were brought to an industry dominated by compliance and regulatory monitoring through the emergence of fintech (Ryu, 2018).

To provide sustainable financial products with secure regulatory process automation, it is essential to offer trustworthy FinTech solutions that combine RegTech innovation.

FinTechs are legal entities with an array of different business models, indicators, and dangers. RegTech enables FIs to analyze compliance, internal control, and accountability for risk data while also enabling effective administration of rules and processes among the many intervention areas (Miklosik, Kuchta, Evans & Žák, 2019).

The supply of financial services using fintech technology is intended to be competitive with the use of conventional financial means. The four core components of fintech are big data, cloud computing, blockchain technology, and artificial intelligence. Fintech, a growing economic sector, uses technology to improve financial operations. (Mohamed & Ali, 2021) Technologies to improve public access to financial services include using smartphones for mobile banking, investing, borrowing, and cryptocurrencies. Start-ups, well-established FinTech companies, and technology firms that hold expertise in

the financial sector compete to replace or improve upon the financial services of established financial institutions. (Buckley, Arner, Zetzsche & Selga, 2019).

Financial institutions are still using antiquated systems that are ill-equipped to manage today's automated and digital financial needs. Financial institutions start turning to RegTech solutions as the expenses of complying with regulatory standards rise to fulfill their regulatory duties and keep up with client requests (Packin, 2018).

FinTechs can cooperate with RegTech providers or with regulatory consulting firms to deliver comprehensive solutions and handle issues with distributed compliance teams. Financial institutions will likely make use of any RegTech that can add insight to data while requiring less manual labor. Finding efficient means to have a technology solution understood, approved, and deployed is a problem that needs to be resolved as soon as feasible. Online identity verification solutions, for instance, can provide users with access to a variety of trustworthy and impartial data sources, such as public records, utility bills, and credit reports. The examples of various partnerships are provided below.

How secure the financial industry and FinTech products and services are is called into question by this paradigm shift in financial rules in the age of technology-enabled finance. This is where cybersecurity comes into the picture (Mosteanu & Faccia, 2021).

The various cyber threats for FinTech companies are:

Malware – Malicious software, viruses, ransomware, worms, and spyware are some examples. When a user clicks on harmful links or visits a rogue website, malware is installed: (Uddin, Ali, & Hassan, 2020).

- Access to critical network components is restricted.
- Additional malicious software could be installed.
- Particular sections can be disrupted by deactivating the system.

Information can be copied by silently copying data from the hard drive (spyware) (Sahrom, Selamat, Ariffin, & Robiah, 2018).

Emotet – A high-level, isolated financial trojan that primarily acts as a downloader or dropper for other financial trojans is referred to as an "emotet" by the CISA.

Denial of Service (DOS) – Denial of Service is a digital attack in which a computer or organization is bombarded with requests and unable to reply.

Man-in-the-Middle (MITM) – A Man in the Middle Programmers inserting themselves into a two-party communication is known as a (MITM) attack.

Phishing – Phishing is an attempt where the attacker sends an email to the targets with the expectation they click on the link in the email. These emails are crafted to look enticing in a bid to make the receiver click on the link. Once the link is visited, a malicious bug tries to infiltrate the system and access the data which is usually used to seek ransom sold to competitors or leaked over the dark web.

SQL Injection – SQL injection is a digital attack involving embedding destructive code in a server using SQL. When data is corrupted, the server deletes it. Malicious code can be added as quickly as typing it into a susceptible website's search field (Mark, 2017).

All these threats can have a massive impact on companies, leading to data and financial loss. FinTech companies must avoid these attacks. This can be achieved by educating the employees about the importance of cybersecurity, ensuring endpoint security by keeping software and systems up to date, setting up a firewall, and taking backups of the data at regular intervals. Also, to mitigate the threats, one must keep an eye out for potential security threats, create countermeasures, and teach the employees what to look for and how to spot them. (Soomro, Shah & Ahmed, 2016).

Although numerous well-known compliance frameworks exist, such as GDPR or PCI DSS, financial service providers have more regulatory requirements than their counterparts in other sectors. For instance, the PCI DSS mandates financial organizations install intrusion detection systems to stop breaches from spreading or going unnoticed. Given the increased compliance standards for financial service providers, it becomes essential to consider a cybersecurity plan to safeguard the company in line with these standards. (Yew & Talib, 2018)

III. RESEARCH METHODOLOGY

A. Data Collection Methods

This research used a mixed-methods approach to data collection, including:

- *Literature Review:* A comprehensive literature review was conducted to understand the existing body of knowledge on FinTech, RegTech,

cybersecurity, and risk management. This was done by searching relevant academic databases and grey literature sources.

- *Expert Interviews:* Semi-structured interviews were conducted with experts in FinTech, RegTech, cybersecurity, and financial regulation. The interviews were used to gain insights on the challenges and opportunities associated with these fields, as well as best practices for managing compliance, risk management, and cybersecurity.
- *Case Studies:* Case studies of FinTech companies that had been successful or unsuccessful in managing compliance, risk management, and cybersecurity were conducted. The case studies were used to identify key factors that contributed to success or failure in these areas.

B. Data Collection Methods

The following data analysis methods were used:

- *Content Analysis:* The literature review data was analyzed using content analysis to identify key themes and trends. This was done using a coding framework that was developed specifically for this research.
- *Qualitative Data Analysis:* The expert interview and case study data were analyzed using qualitative data analysis methods, such as thematic analysis and grounded theory. This was done to identify patterns and insights that could be used to answer the research questions.

C. Research Design

The research design was a sequential mixed-methods approach. This meant that the literature review and expert interviews were conducted first, followed by the case studies. This allowed for the findings from the literature review and expert interviews to be used to inform the case study selection and data collection.

IV. RESULTS, DISCUSSIONS AND SOLUTIONS

Increased resource allocation for compliance and security activities would seem to be the obvious solution to this problem, but this is easier said than done. To ensure a thorough knowledge of the most important topics, open talks at the board level are required. This includes the potential costs of security breaches or fines for noncompliance, as well as the fact that good security and compliance policies can significantly contribute to supporting rather than detracting from business aspirations (Guo, Sriram & Manchanda, 2021).

Engaging other institutions and regulators to test and scale solutions more quickly and at lower cost and risk is part of a successful RegTech strategy. As an illustration, the creation of shared testing facilities for solutions that automate the management of the impact and changing of regulations. RegTech will assist financial institutions in collaborating with financial institutions and FinTechs to quickly scale solutions. In many ways, the contemporary economy is supported by banks and other financial organizations. They provide an extensive array of financial offerings, which encompass services like lending, transaction handling, ensuring valuable assets, and various others (Magnuson, 2018).

At the same time, they are under more and more pressure to abide by rules, safeguard private information, and stop fraud. Without using some kind of automation, it is practically difficult for financial institutions to adhere to current regulatory requirements in practice.

A. Categories of RegTech

Although there is no agreed-upon method for classifying regulatory monitoring solutions, RegTech can be divided into the following eight groups (Adeyoju, 2021).

- *Identification of the Client* - This collection of regulatory solutions aids in the collection and processing of client data by financial institutions. This includes procedures like Know Your Customer (KYC) and Anti-Money Laundering checks.
- *Watching* - This branch of regulatory technology focuses on keeping track of ongoing transactions to see if they violate rules or exhibit any suspicious behaviour.
- *Reporting* - This category aids businesses in meeting their regulatory reporting requirements. To the appropriate authorities, internal data must be gathered, processed, and sent.
- *Data Security* - These compliance technologies provide a broader level of protection against data breaches and cybersecurity risks while protecting

personal data by laws like the GDPR.

- *Analytics and Data Warehousing, Number* - Companies can correctly store, classify, and analyze the enormous amounts of data needed for legal compliance with the aid of this regulatory technology.
- *Analysis of Laws and Regulations* - To assist financial institutions in identifying gaps or instances of non-compliance in their internal structure, this phrase refers to technology that monitors and interprets any current and emerging legislation.
- *Education* - This package of resources is intended to assist financial institutions in informing and educating their staff about the laws and regulations pertinent to their job duties.
- *General Compliance* - All regulating technology that doesn't fit cleanly into one of the aforementioned descriptions is included in this catch-all category. It covers things like risk modelling and forecasting. (Conti, Dargahi & Dehghantanha, 2018).

The main lesson to be learned from this is that no one RegTech solution can meet all compliance needs. Instead, financial businesses often choose several options to put up a toolkit that addresses their unique organizational requirements. Due to the sensitivity of the finance sector, many businesses require compliance with certain laws and regulatory frameworks before doing business. A new pool of opportunities might be opened up by becoming an early adopter in terms of new rules, exhibiting security thought leadership, and obtaining relevant accreditations (Zhao, Fa & Hu, 2014).

With the new advancements in technologies, FinTechs face new cyber threats like malware. To prevent malware from spreading within the FinTech organization, one should implement:

- *Security Software* - It is a crucial component of our virus protection, even though it is not the entire answer. Using antivirus, anti-malware, anti-ransomware, and other anti-exploit tools, it guards the network and its features against the initial infection of a malware attack (Barrell & Davis, 2011).
- *Passwords and Multi-Factor Authentication* - Managing passwords and implementing multi-factor authentication are crucial aspects of cybersecurity. It's essential to refrain from jotting down passwords in easily accessible locations. Given the complexity of managing numerous credentials, a password manager can be employed for efficient management of login information. Additionally, incorporating multi-factor authentication adds an extra layer of security, thwarting potential privilege escalation during the initial phases of malware infiltration.
- *Employee Education* - Every network user, regardless of their direct engagement in security, plays a crucial role in protecting a FinTech organization against cybercrime. Their level of cybersecurity awareness, though, will determine how effective they are in this position. By holding frequent training sessions that cover these crucial subjects, a FinTech company may efficiently increase the size of its security team and improve the company's security posture. Cyber-attackers send phishing emails that look like they are from the company asking for personal information to gain access to restricted areas. The links usually are made to look legitimate or authentic, so the employees fall prey to the attackers' malpractices.
- Employee training is among the most efficient ways to safeguard against cyberattacks and other data breaches.
- *Updating software and System* - Cyberattacks happen because the system or software is not entirely updated, leaving them vulnerable. Cybercriminals use these loopholes and take advantage to gain access to your network. Hence, all the systems and software must be updated.
- *Ensure Endpoint Protection* - It helps protect networks remotely bridged to devices. These network paths need to be covered with specific endpoints.
- *Establish a Firewall* - When using the internet while operating, the data firewall must be on so that no harmful threats can track and access your data.
- *Backup of data* - It will come in handy if your data is corrupted or formatted incorrectly. To secure your data and privacy, one must always have a backup of the data.
- *Monitoring reaches the System* - Because one of the attacks on the framework can be physical, it's critical to keep track of who has access to your network. Someone may just stroll into your workplace and put a USB to corrupt your data or put a virus in the

system allowing it to infiltrate or contaminate your entire firm.

- *Wireless Fidelity Security* - Getting Wi-Fi secured is perhaps the most important thing one can accomplish. With the increase in the number of devices connecting with the network and using Wi-Fi, the number of threats has also increased.

The various ways in which threats can be mitigated are:

- *Be On the Lookout for Security Threats* - Attackers are continuously developing their techniques and methodologies to deliver the best measure of likely damage that could be expected. One should constantly keep an eye out for new threats and keep up with the industry's headlines. Interact with others in the association and market to find out how things are doing. On the other hand, sharing such information with companions is good IT hygiene. Security is a collaboration across workers, groups, associations, and businesses.
- *Create Your Countermeasure* - Changing (or disabling) the server's configuration options might mitigate some of the dangers, ensuring that the impacted center programming is rectified and a firewall rollout can also be prepared. The threats such as denying a port permission to send or receive traffic through the company should also be addressed.
- *What to Look for and Spot It* - Clients can be the best data security asset accessible when specific, and strategy materials are used effectively. The workers are the top line of protection in recognizing whatever might cause damage to any private or business resources. Therefore, cyber-attacks can be massively reduced if they know what and where the problems might occur.

V. IMPLICATIONS

Organizational implications

- *Reputation* - When a company suffers a cyber-attack, people lose faith and confidence in it and are hesitant to invest more in it.
- *Intellectual Property Theft* - An organization's intellectual property, such as a patent, copyright, or trade secret, can be stolen, causing significant damage.
- *Loss of Sensitive Business Information* - Important business data should be secured, as its loss can be costly to the company because it might be sold to competitors, leaked online, or used for ransom.
- *Lack of Trust* - Users lose faith in the organization after a cyber-attack. Customers are forced to switch to other providers due to the company's actions.
- *Business Disruption/Sales Expenses* - Cyber-attacks can harm business or sales. Customers facing service attacks will be unable to use the service, resulting in a significant loss for the company in a short period.
- *Malware Damage* - Malware can sometimes wipe out entire networking equipment, forcing a company to pay a lot of money to replace them.
- *Stock Prices* - Malware could be used to define an organization's stock prices to lower the value and reputation of that FinTech organization (Pant, 2020).

VI. LIMITATIONS AND FUTURE RELEVANCE

A lack of a comprehensive high-level security strategy can be problematic for some financial institutions. This deficiency may arise due to a failure to take cybersecurity seriously or a perception that it is a low-priority concern. However, having a well-defined high-level strategy is crucial for achieving security goals and effectively preventing and mitigating cyberattacks.

Furthermore, if a network is inadequately secured, it becomes relatively simple for malicious actors to gain unauthorized access to a system. Once they breach the network, they can potentially infiltrate and compromise various devices and systems connected to it.

Studies on AI and NLP should be carried out to understand behavioral analytics which will help ensure the integrity of the systems. Organization patterns can be studied to come up with better security solutions. Future research on understanding how the operations are carried out can help improve the security of Fintech companies (Kazi & Prabhu, 2015).

VII. CONCLUSION

The financial sector's digital transformation was accelerated by the post-crisis reforms, which saw the introduction of new products, services, and business models based on the most recent technical advancements (Barrell & Davis, 2011).

Fintech is expanding more quickly than ever before and has revolutionized the financial markets through innovation and technology. Digital finance is now emerging as the backbone of businesses. It has a bright future, but it also faces more restrictions, fines, and legal measures (Pant, 2020).

In essence, better processes do more than just reduce the expensive risks of penalties or violations. They can also endeavor to improve procedures and open up new possibilities. The benefits will start to be realized by integrating RegTech and cybersecurity into the core of any digital transformation strategy and establishing a management-level knowledge of the advantages.

In this context, RegTech is not simply a tool; it is an absolute requirement. With the help of these solutions, businesses may operate legally, avoid expensive mistakes, and simplify internal procedures. All while assisting them to reduce expenses, and remain adaptable and responsive.

With so much reliance on the internet today, online security is one of the world's greatest needs. Network security risks are hazardous to the safety of any financial organization. Employees and FinTech companies need to constantly update their framework and organization's security settings and educate the public to use legitimate antivirus software so that organizational security settings stay free from these threats. Information plays a critical role in the commissioning of numerous cybercrimes and vulnerabilities (Treleaven, 2015).

Fraud, regulatory complexity, and risks to cyber security do not go away. They may even continue to expand in the future. As a result, RegTech and cybersecurity both are essential for a contemporary financial institution.

REFERENCES

Adeyoju, A. (2021, November). Cybercrime and cybersecurity: FinTech's greatest challenges. *SSRN Electron*. J., 1-5. doi:10.2139/ssrn.3486277

Arner, D., Zetzsche, D., Buckley, R., & Barberis, J. (2017, January). FinTech and RegTech: Enabling innovation while preserving financial stability. *Journal of International Affairs, 18*(3), 47-58.

Barrell, R., & Davis, E. P. (2011, April). Financial regulation. *Natl. Inst. Econ*. Rev., *216*, 4-9 doi:10.1177/0027950111411368

Buckley, R., Arner, D. W., Zetzsche, D., & Selga, E. (2019, January). The dark side of digital financial transformation: The new risks of fintech and the rise of TechRisk. *SSRN Electronic Journal*. doi:10.2139/ssrn.3478640

Conti, M., Dargahi, T., & Dehghantanha, A. (2018, August). Cyber threat intelligence: Challenges and opportunities. Adv. *Inf. Secur., 70,* 1-6. doi:10.1007/978-3-319-73951-9_1

Guo, T., Sriram, S., & Manchanda, P. (2021, October). The effect of information disclosure on industry payments to Physicians. *J. Mark. Res., 58*(1), 115-140. doi:10.1177/0022243720972106

Kazi, R., & Prabhu, S. (2015). Management of service gaps by infusion of technology. *Telecom Business Review*, *8*(1), 17-21. Retrieved from http://www.publishingindia.com/tbr/65/management-of-service-gaps-by-infusion-of-technology/407/2878/

Lee, I., & Shin, Y. J. (2017, October). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, 35-46. doi:10.1016/j.bushor.2017.09.003

Magnuson, W. (2018). Regulating fintech. *Vanderbilt Law Rev.*, *72*(4), 1167-1226. Retrieved from scholarship.law.vanderbilt.edu/vlr/vol71/iss4/2/

Mark, C. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *J. Risk Manag. Financ. Institutions*, *10*(2), 196-200. Retrieved from ideas.repec.org/a/aza/rmfi00/y2017v10i2p196-200.html

Miklosik, A., Kuchta, M., Evans, N., & Žák, Š. (2019, June). Towards the adoption of machine learning - Based analytical tools in digital marketing. *IEEE Access, 7,* 85705-85718. doi:10.1109/ACCESS.2019.2924425

Mohamed, H., & Ali, H. (2021, January). Finding solutions to cybersecurity challenges in the digital economy. *Fostering Innovation and Competitiveness With FinTech, RegTech, and SupTech*, 80-95. doi:10.4018/978-1-7998-4390-0.ch005

Mosteanu, N. R., & Faccia, A. (2021, January). Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation. *J. Open Innov. Technol. Mark. Complex,* 1-19. doi:10.3390/joitmc7010019

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021, March). Fintech firms and banks sustainability: Why cybersecurity risk matters? *International Journal of Financial Engineering*, 1-14, 2150019. doi:10.1142/s2424786321500195

Packin, N. (2018, March). RegTech, compliance, and technology judgment rule. *Chi.-Kent L. Rev*., *93*(1), 193.

Pant, S. K. (2020). Fintech: Emerging trends. *Telecom Business Review*, *13*(1), 47-52.

Ryu, H. S. (2018, January). Understanding benefit and risk framework of Fintech adoption: Comparison of early adopters and late adopters. *Hawaii International Conference on System Sciences,* 3864-3873. doi:10.24251/hicss.2018.486

Sahrom, M., Selamat, S. R., Ariffin, A., & Robiah, Y. (2018, April). Cyber threat intelligence – Issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science,* 371-379. doi:10.11591/ijeecs.v10.i1

Schueffel, P. (2016, December). Taming the beast: A scientific definition of Fintech. *Journal of Innovation Management*, *4*(4), 32-54. doi:10.2139/ssrn.3097312

Soomro, A. Z., Shah, M. H., & Ahmed, J. (2016, April). Information security management needs more holistic approach: A literature review. *Int. J. Inf. Manage.*, *36*(2), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009

Pant, S. (2020) Fintech: Emerging trends. *SSRN*, 47-52. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3763946

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020, January). Cybersecurity hazards and financial system vulnerability: A synthesis of the literature. *SSRN Electron, 22*(4), 239-309. doi:10.1057/s41283-020-00063

Yew, C. Y., & Talib, A. (2018, April). A review of Fintech regulations in China, Singapore, and Hong Kong. *J. Econ. Bus., 1*(1), 43-56. doi:10.31014/aior.1992.01.01.5

Zhao, J. L., Fan, S., & Hu, D. (2014, July). Business challenges and research directions of management analytics in the big data era. *J. Manag. Anal., 1*(3), 169-174. doi:10.1080/23270012.2014.968643