Frist class
ASSIGNMENT SERVICE
that you deserve

DR KHANH
Writing Service

SAMPLE FOR ASSIGNMENT 70+DI

From Dr.Khanh Assignment Service

THÔNG TIN LIÊN HỆ :

DrKhanhAssignmentService
www.drkhanh.edu.vn
(+84) 939 070 595 hoặc (+84) 348 308 628

DR KHANH
Writing Service

One stop-solution for your academic stress

Essay Writing

Professional writers craft custom essays tailored to your specific requirements and academic standards.

- Plagiarism-free guarantee
- Timely delivery
- Expert writers in diverse subjects

Assignment Assistance

Expertly crafted helps for all tasks.
Consultation services where experts provide guidance on understanding assignment requirements, brainstorming ideas, and structuring your work.

- Clarification of assignment instructions
- Brainstorming sessions
- Topic suggestions

Dissertation & Thesis Help

Specialized guidance for graduation and research projects.
Comprehensive assistance for thesis and dissertation writing, from topic selection to final draft refinement.

- Access to scholarly sources
- Formatting adherence
- Data analysis support

Proofreading & Editing

Professional refinement of papers.

- Grammar and spelling correction
- Style improvement
- Formatting assistance

Online Tutoring Sessions

Personalized support to boost understanding.
One-on-one tutoring sessions conducted online to help students grasp difficult concepts and improve their grades.

- 24/7 availability
- Step-by-step explanations
- Experienced tutors
- Interactive whiteboard tools
- Flexible scheduling

Exam Preparation

Prompt aid for all subjects.
Resources and guidance to help students prepare for exams, including study guides, practice tests, and exam-taking strategies.

- Subject-specific study materials
- Mock exams
- Time management tips

Financial Markets and Institutions

ASSIGNMENT COVER PAGE

Assignment 3 – Individual research project

Course ID	**BAFI3182: Financial Markets**
Campus	**SGS Campus**

ASSIGNMENT 3: To what extent does cybercrime influence the dynamics of the modern financial market today and its effects?

Table of Content

Abstract:

Virtualization has increased due to the use of the Internet and cyberspace for business processes, notably in the financial industry. Cybercrime has increased with platform reliance. This conceptual document examines how cybercrime affects financial technology, stock, and bond markets. This study examines the main causes of financial cybercrime. To conclude, cybercrime is driven by the potential gains from accessing valuable financial institution data, the relatively lenient penalties for such offenses, and the lack of legal consistency. According to the research, financial technology trust and cybercrime frequency are negatively correlated. Cybercrime is hindering cryptocurrency adoption. Cybercrime and stock and bond returns are examined in the research to go beyond financial market patterns. Cybercrime is linked to stock and bond price declines.

Introduction:

The contemporary global economy is progressively dependent on online transactions, online databases, and digital communication. Consumers worldwide are transitioning their consumption habits to the digital realm (Omoola 2016). As the pace of this phenomenon quickens and the degree of interconnectivity deepens, malevolent assaults of diverse types and magnitudes aimed at purloining identities, financial data, and other varieties of personal information, as well as confidential institutional information, are increasingly becoming a normative aspect of contemporary existence (Rubini 2019). Cybercrimes encompass a diverse range of illicit activities that employ information and communication technology. This phenomenon is not of recent origin; rather, it has been extant for a considerable duration. The financial sector has been significantly impacted by the internet, which has both empowered and disrupted many organizations. However, this has also made it a prime target for cybercriminals, posing a significant challenge for the industry. Undoubtedly, the banking industry possesses all the necessary components for a comprehensive cybercrime strategy. Financial institutions possess invaluable data, encompassing individuals' financial accounts and identification particulars (Taplin 2016). The proliferation of cybercrime poses a significant threat to the financial markets across various aspects and functions. To what degree and by what means does cybercrime affect the financial sector and its various components? Equity market and bond market are main 2 aspects that this paper address.

The article initially provides a concise overview of the main factors contributing to the rising incidence of cybercrime targeting the financial industry. Subsequently, it examines the impacts of

cybercrime on the financial technology industry first; followed by equity and bond markets as mentioned above. Subsequently, the study proceeds to investigate a pair of research inquiries by conducting a comprehensive examination of previous literature on relevant topics.

1. How cybercrime affects financial technology (Fintech)?
2. How cybercrime affects stock and bond markets?

Literature review

a. The underlying factors of cybercrime that impact organizations, particularly the financial industry

➢ The growing dependence of the banking industry on the Internet

Innovative and cost-effective methods are being used to make funding easier for businesses (Bonnassies 2023). Electronic finance uses technology to communicate and distribute financial goods and services through the Internet. Modern financial services use the e-channel. Online banking, payment processing, brokerage services, mortgage and other loan providing, insurance, and other related services are included (Martin 2017). Electronic money has grown globally due to the Internet. Convenience, transparency, knowledge, and cost savings are the benefits (Oseni and Ali 2019). Internet-enabled gadgets let people trade financial markets from anywhere. Cyberspace, where technology drives cybercrime, hosts the above activities (Chen et al. 2019). Due of their public access, sensitive data, and money, financial institutions are often attacked. Thus, these companies, particularly financial institutions, are more vulnerable to cyberattacks, which are motivated by profit, data theft, or customer disturbance (Ahmed et al. 2018).

➢ The expenses associated with criminal activities are comparatively lower than those of conventional crimes

Cybercriminals obtain less sentences, arrests, and prosecutions than traditional criminals. Due to the high expense of jail for the government and the opportunity for networking and information sharing among criminals, cybercrime is often punished simply financially. Due to many circumstances, financial identity theft cases seldom involve law enforcement. According to the Federal Trade Commission (FTC), many victims of bank account theft immediately contact their financial institution to remedy the issue rather than reporting it to police authorities (Baker and

Robinson 2020). Even after being victimized by crime, institutions may hesitate to contact law enforcement due to fears about negative publicity and data breach. Due to their lack of technological understanding, law enforcement may be reluctant to believe claims of minor cyber-attacks. They may also see the lending institution as the victim, lowering the likelihood of financial sector cyberattacks (Alexandrou 2022).

- **The lack of consistency and clarity in the laws**

Despite global cybercrime laws, banking institutions struggle to enforce them. Cybercrime is plagued by a lack of clarity on what constitutes cybercrime and its legal meaning. Cybercriminals' identities and IP addresses are difficult to determine due to unrestricted access to information and communication and the right to hide from Internet service providers (Peersman et al. 2016). Anonymity problems promote cybercrime and undercut cybercrime policies. Cybercriminals may avoid prosecution by operating outside the targeted bank's jurisdiction and using stolen bank login credentials or phishing. National procedural rules vary, making transnational cybercrime investigations difficult. Thus, even if the culprits are recognized, they may avoid punishment without extradition or joint legal counsel (Nguyen et al. 2022).

b. Cybercrime affects financial technology

According to Stewart and Jürjens (2018), the concept of data security in this particular context pertains to the guarantee of maintaining the confidentiality of financial data and its crucial assets, including the equipment utilized for the purpose of collecting, storing, and transmitting data. Hence, apprehensions regarding the matter encompass both personal data and action-oriented predicaments that patrons evaluate in accordance with the degree to which technology vendors exhibit readiness and competence in safeguarding their monetary data against possible cyber threats (Taherdoost, 2018). The concerns surrounding the adoption of technology, specifically FinTech (de Luna et al. 2019), mobile payments (Chan et al. 2022), and e-commerce (Rahayu, & Day et al. 2017), are a major hindrance to its implementation.

Yu (2016) reported that a majority of individuals in Taiwan, more than 56%, exhibit reluctance towards the adoption of mobile banking due to apprehensions regarding security. According to Gimigliano (2016), a significant proportion of banking institutions in the European Union, specifically 71%, regard cybersecurity as the primary obstacle that hinders their collaboration with FinTech companies. This apprehension stems from the potential harm that may arise from

cybercrime as a result of such partnerships (Gordan et al. 2022). It is argued that the increase in cybercrime has emerged as a significant impediment to the widespread acceptance of FinTech, as many consumers associate this security issue with a feeling of discomfort. The adoption of fintech has been impeded by security concerns, as evidenced by previous research (Chan et al. 2022). The protection of personal data confidentiality and security has been crucial to the successful execution and handling of financial transactions (Friend et al. 2020). Consequently, the unanticipated misappropriation or breach of individualized information leads to unfavorable attitudes and impedes the uptake of financial technology.

To clarify, there exists a negative correlation between the implementation of Financial Technology (FinTech) and concerns regarding security due to the increasing prevalence of cybercrime.

c. Cybercrime affects stock market and bond market

With regard to **stock market**, the adverse effects of news headlines pertaining to cybercrime on the stock values of firms that are publicly listed were observed, with the statistical significance of the impact being evident after a period of three days. The Dow Jones Industrial's average fluctuations in stock prices were observed to be 0.31%, 0.38%, and 0.33% on days 1, 3, and 7, respectively, subsequent to the release of statements pertaining to cybercrime. The aforementioned observation aligns with the research conducted by (Mthembu et al. 2022), which revealed that financial sector enterprises exhibited a tendency to react to cybercrime in an aggregated manner over a span of three days, as opposed to enterprises operating in other industries. Iyer et al. (2020) conducted research that further elaborates on the subject. Their findings indicate that the returns of the stock market in the financial sector exhibit more negative trends compared to other sectors even before the occurrence of cybercrime. This implies that insider trading is a probable outcome of cybercrime. Specifically, The Securities and Exchange Commission (SEC) has recently emphasized in a report (Securities Exchange Commission, 2018) that corporations should incorporate an assessment of cyber safety in the board's discussion and analysis section. Additionally, the report suggests that corporations should disclose all measures adopted to enhance their cyber defenses. Historically, the Securities and Exchange Commission (SEC) has emphasized the importance of promptly revealing unfavorable cyber occurrences. Equifax, a company that experienced a widely publicized cyberattack, disclosed in September 2017 that 143 million of its customers were affected. The breach was notable for the fact that insiders were aware of it for over a month but did not choose to reveal it. Despite the findings of Rosati et al. (2017) indicating the

absence of informed market participants through abnormal trading activity, certain insiders were observed to have engaged in trading activities leveraging their internal knowledge, resulting in significant profits. The Securities and Exchange Commission (SEC) issued a report on February 26, 2018, in which it advised individuals with insider knowledge to refrain from engaging in trading activities that rely on the acquisition of information obtained through cyberattacks (). It is suggested that insiders tend to divest their stocks when their organization opts to conceal information pertaining to cybercrime from investors. However, corporations that voluntarily disclose such information tend to observe a reduced tendency among insiders to sell their shares while the event remains undisclosed (Kumar et al. 2021).

Furthermore, financial institutions tend to encounter comparatively more adverse stock market repercussions in contrast to other enterprises operating in diverse sectors. It is unsurprising that financial institutions, including banks, are tasked with safeguarding their systems, networks, and financial assets, as well as ensuring the protection of customer data (Roškot et al. 2021). Nonetheless, in the event of a disclosure of a cybercrime to the public, the impact on the stock prices of technology companies is generally limited. Corbet et al. (2019) suggest that this could be attributed to the fact that these enterprises often possess the necessary resources and expertise to promptly address and minimize the potential negative impact of criminal activities.

Moving on to **bond market**, the study reveals that the bond markets exhibit no immediate response during the event window of short duration. Nevertheless, bondholders experience a substantial decline in value over an extended period encompassing the public disclosure of a cyberattack. On average, bond holders encounter a negative return of roughly 2% within a one-month timeframe (Castells 2021).

On a regular basis, when analyzing the adverse bond returns of the affected parties in these incidents in comparison to a comparable publicly-traded company that did not experience a similar attack, the adverse return is also roughly 2% and the economic impact of each bond is significant (Chua 2017). At present, the scope of cyber insurance policies does not extend to indemnifying losses incurred in the form of depreciation in the value of stocks or bonds. The potential advantages of cyber insurance covering the majority of operational losses and legal expenses are primarily enjoyed by stockholders and bondholders. However, they do not receive any compensation for the depreciation in value of their financial holdings .

Despite such drawbacks from cybercrime, a mere 23% of negative cyber occurrences are disclosed voluntarily by corporations in their public declarations. The present study's results are supported by a recent article in the Wall Street Journal (US SEC 2018), which reveals that despite the Securities and Exchange Commission's (SEC) diligent efforts, a considerable number of cyberattacks remain unreported. Firms that fail to disclose adverse cyber events and provide insufficient disclosures are potentially providing investors with inaccurate information regarding the negative consequences. As a consequence, there may be inaccurate assessments of the equity and debt securities of the company. Subsequent investigations may delve into the scope of insufficient disclosures or lack of disclosures, along with associated corporate measures that may indicate substandard corporate governance and entrenched management with regard to cyber assaults.

Conclusion

To conclude, the study investigated how cybercrime affects Fintech, one of the most important financial movements, followed by stock and bond markets and equity markets. Cybercrime is increasingly concentrated in the banking industry due to regulatory inconsistencies and its low-risk, high-profit potential. Cybercrime also discourages financial technology usage. Cybercrime may lower stock prices and profits. Bond markets exhibit little short-term response. Despite the risk to bondholders, corporations report cybercrime instances. Due to the serious consequences of cybercrime, such risks are crucial. Given the increasing reliance of businesses across sectors on the Internet and cyberspace for their operations, it is crucial that they, particularly those in the financial sector, equip themselves with robust cybersecurity measures and control systems to protect against cybercrime.

Limitation

One of the constraints associated with analyzing the enduring consequences of unfavorable cyber incidents pertains to the imperfect nature of disclosures concerning such events. Moreover, the research outcomes just derive from academic journals without collecting any data for running regression model for demonstrating relationship, hence a ‘biased’ research result based on previous findings. On top of that, there are many types of stock markets as well as bond markets, but this paper not really addresses all of these in details. Thus, it is recommended further research would investigate more deeply into each type of each market.

Part B: Reflection on industry talk

Financial market history is first covered by the speaker. Internet transactions enable online marketplace transactions. Financial markets include foreign markets, money markets, stock markets, bond markets, and commodities markets. After the sharing section, I researched these markets. Global currency exchange rates are determined by the FX markets. Markets for currency pairings include buyers, sellers, exchangers, and speculators. Short-term debt investments are traded on money markets. Large wholesale transactions are made by institutions and enterprises. Bank depositors and money market mutual fund investors are covered. Stock trading is the purchasing and selling of publicly traded corporation shares. Financial transactions occur on exchanges and regulated OTC markets. Buy, sell, and trade on commodity marketplaces exchange basic items. Coffee, corn, and agricultural goods are popular in Vietnam. The 10-year commodities market's promise to provide Vietnam a competitive edge, notably for coffee roasters, has made it popular in Vietnam.

Through foreign exchange and international payment systems, the financial market enables trade and business. The speaker giving an example of an individual's limited productivity potential and rising needs for other commodities to improve their level of life. Selling things for money involves international currency markets to swap value. Financial markets allocate capital via bond markets, mostly government and corporate bonds. This method is effective. Socioeconomically diverse people share living spaces in modern society. Wealthy people don't need more money to invest to enhance their quality of life. Therefore, people with higher socioeconomic position would lend to those with lower socioeconomic status for interest to make a profit. Government and business bonds are traded on the bond market. The financial market's third purpose is hedging and insurance. To reduce the effect of commodity market price changes, a hedging strategy involves entering into a contractual arrangement to sell commodities at a pre-determined price point.

Banks' function in financial markets is then discussed by the guest professor. Corporations and governments issue bonds. This increases liquidity risk, which is the capacity to pay bondholders. Therefore, to limit corporate bond risk, which emerges as corporations defaulting on bond payments to investors. Financial transactions between fund providers and fund recipients are made possible by banks. Economic development is promoted by financial institutions.

The following shows Fx counterparty turnover. This trait is seen in 48% of financial firms. Institutional investors and non-reporting banks make up 45% and 23% of financial institutions,

respectively. As the guest speaker noted, the opposition wants the government to adopt either an expansionary or contractionary economic strategy.

The speaker closes with a government bond market view. Government bonds provide long-term investment prospects, unlike the money market, which focuses on short-term liquidity. Thus, the topic is irrelevant for individual investors who may require cash for sickness. Second, the government bond market's minimum investment requirement of 30 to 50 billion dollars makes it unsuitable for ordinary investors. Since such a large quantity of funds is usually only available to wealthy individuals, they may not consider this investment option. Corporate bonds attract individual investors due of their better yields and accessibility. Government bonds are purchased by few people. Financial institutions may buy foreign government bonds, including US ones.

Reference

Ahmed S, Youngdoo Lee, Seung-Ho Hyunand Insoo Koo. (2018). 'Feature Selection-Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning', *IEEE Access*, 6, 27518–27529, doi:10.1109/ACCESS.2018.2835527

Alexandrou, A. (2022) 'Cybercrime and Internet technology : theory and practice - the computer network infrastructure and computer security, cybersecurity laws, internet of things (IoT), and mobile devices', *Boca Raton, Florida ;: CRC Press.*

Baker, D. J. & Robinson, P. H. (2020) 'Artificial Intelligence and the Law : Cybercrime and Criminal Liability', *Milton: Taylor & Francis Group*.

Bonnassies, O (2023) *Fund to Finance Gryphon A319 Acquisitions*." Airfinance Journal, 2023.

Castells D (2021) *Cybercrime stokes costs for small lenders; Asian banks' bond issuances stay low.* SNL Financial Extra.

Chan R, Troshani, I., Rao Hill, S.and Hoffmann, A. (2022). 'Towards an understanding of consumers' FinTech adoption: the case of Open Banking', *International Journal of Bank Marketing*, 40(4):886–917, doi:10.1108/IJBM-08-2021-0397

Chan R, Troshani, I., Rao Hill, S.and Hoffmann, A. (2022) 'Towards an understanding of consumers' FinTech adoption: the case of Open Banking', *International Journal of Bank Marketing*, 40(4):886–917, doi:10.1108/IJBM-08-2021-0397

Chen X, Liu, C.and Li, S. (2019). 'The role of supply chain finance in improving the competitive advantage of online retailing enterprises', *Electronic Commerce Research and Applications*, 33, 100821–, doi:10.1016/j.elerap.2018.100821

Chua R(2017*). Monday's headlines, Financials edition*. SNL Financial Extra.

Corbet S & Gurdgiev, C. (2019). 'What the hack: Systematic risk contagion from cyber events.', *International Review of Financial Analysis*, 65, 101386–, doi:10.1016/j.irfa.2019.101386

de Luna T, Liébana-Cabanillas, F., Sánchez-Fernández, J.and Muñoz-Leiva, F. (2019). 'Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied', *Technological Forecasting & Social Change*, 146, 931–944, doi:10.1016/j.techfore.2018.09.018

Friend G, Grieve, L. B., Kavanagh, J.and Palace, M. (2020). 'Fighting Cybercrime: A Review of the Irish Experience', *International Journal of Cyber Criminology*, 14(2):383–399, doi:10.5281/zenodo.4766528

Gimigliano G(2016). 'Bitcoin and Mobile Payments Constructing a European Union Framework (Gimigliano, Ed.; 1st ed. 2016.)', *Palgrave Macmillan UK*, doi:10.1057/978-1-137-57512-8

Gordan F, McGovern, A., Thompson, C.and Wood, M. A. (2022). 'Beyond cybercrime: New perspectives on crime, harm and digital technologies', *International Journal for Crime, Justice and Social Democracy*, 11(1), i–viii, doi:10.5204/ijcjsd.2215

Iyer S, Simkins, B. J.and Wang, H. (2020). 'Cyberattacks and impact on bond valuation', *Finance Research Letters*, 33, 101215–, doi:10.1016/j.frl.2019.06.013

Kumar G, Singh, O. P.and Saini, H. (2021). 'Cybersecurity : Ambient Technologies, IoT, and Industry 4. 0 Implications', *Taylor & Francis Group*.

Martin A (2017). 'Coordinating Modern Cross-Border Financial Services: No Global Policy, No Global Legal Framework, but Some Regional Opportunities', *The International Lawyer*, 50(3):467–502.

Mthembu N, Sanusi, K. A.and Eita, J. H. (2022). 'Do Stock Market Volatility and Cybercrime Affect Cryptocurrency Returns? Evidence from South African Economy', *Journal of Risk and Financial Management*, 15(12):589–, doi:10.3390/jrfm15120589

Nguyen V, Truong, T. V.and Lai, C. K. (2022) 'Legal challenges to combating cybercrime: An approach from Vietnam', *Crime, Law, and Social Change*, 77(3):231–252, doi:10.1007/s10611-021-09986-7

Omoola Sand Oseni, U. A. (2016) 'Towards an Effective Legal Framework for Online Dispute Resolution in E-commerce Transactions: Trends, Traditions and Transitions', *IIUM Law Journal*, 24(1), doi:10.31436/iiumlj.v24i1.236

Oseni, U. A. & Ali, S. N. (2019) 'Fintech in Islamic Finance : Theory and Practice.', *Milton: Taylor & Francis Group.*

Peersman, Schulze, C., Rashid, A., Brennan, M.and Fischer, C. (2016). 'iCOP: Live forensics to reveal previously unknown criminal media on P2P networks', *Digital Investigation*, 18, 50–64, doi:10.1016/j.diin.2016.07.002

Rahayu R and Day, J. (2017). 'E-commerce adoption by SMEs in developing countries: evidence from Indonesia', *Eurasian Business Review*, 7(1):25–41, doi:10.1007/s40821-016-0044-6

Roškot M, Wanasika, I.and Kreckova Kroupova, Z. (2021). 'Cybercrime in Europe: surprising results of an expensive lapse', *The Journal of Business Strategy*, 42(2):91–98, doi:10.1108/JBS-12-2019-0235

Rubini A (2019) 'Fintech in a flash : financial technology made easy (Third edition.)', *Walter de Gruyter Inc.*

Taplin R(2016) 'Managing Cyber Risk in the Financial Sector : Lessons from Asia, Europe and the USA', *Taylor & Francis Group.*

US SEC (2018) *SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls*, SEC, accessed 25 June 2023, https://www.sec.gov/news/press-release/2018-236

Yu C (2016). 'CONSUMERS' RESISTANCE TO USING MOBILE BANKING: EVIDENCE FROM THAILAND AND TAIWAN', *International Journal of Electronic Commerce Studies*, 7(1):21–38, doi:10.7903/ijecs.1375

Frist class
ASSIGNMENT SERVICE
that you deserve

DR KHANH
Writing Service

ƯU ĐÃI 25% CHO FIRST ORDER

Tận hưởng trải nghiệm học tập với DrKhanh Assignment. Đặt hàng ngay hôm nay để nhận được sự hỗ trợ chuyên nghiệp và đạt được thành công trong học tập của bạn!

▶ NHẬN TƯ VẤN MIỄN PHÍ! ◀

Đừng ngần ngại liên hệ với đội ngũ của chúng tôi nếu bạn cần bất kỳ thông tin bổ sung nào hoặc muốn biết thêm về dịch vụ của chúng tôi. Chúng tôi luôn sẵn lòng hỗ trợ bạn!