

Academic Journal of Research and Scientific Publishing

International peer-reviewed scientific journal

The Fifty-fourth Issue

Publication date: 05-10-2023

ISSN: 2706-6495

Doi: doi.org/10.52132/Ajrsp.e.2023.54

Email: editor@ajrsp.com



Dedication

It is our pleasure and great privilege to present the fifty-fourth issue of the Academic Journal of Research and Scientific Publishing to all researchers and doctors who published their research in the issue, and we thanks and appreciate to all contributors and supporters of the academic journal and those involved in the production of this scientific knowledge edifice.

Academic Journal of Research and Scientific Publishing

Publication Date: 05-10-2023 ISSN: 2706-6495



Editorial Board

Chief Editor:

Prof. Dr. Khetam Ahmed Al-Najdi

Advisory Members:

- Dr. Aicha abdelhamid eltteli abdelhamid
- Prof. Dr. Riad Said Ali Al-Mutairi

Editorial Members:

- Dr. Azab Alaziz Alhashemi
- Prof. Dr. Khaled Ibrahem Khalil Hijazi Abu Alqumsan
- Dr. Abu Obida Taha Gebreel Ali
- Dr. Badreddine Berahlia,
- Dr. Zainab Ridha Hammoodi Aljwaid,
- Dr. Basma Mortada Mohamed Foda
- Dr. Wisal Ali Al-hommada
- Dr. Bilal Khalaf Ali Alzboun
- Dr. Tameem Mosa Alkrad,
- Dr. Walaa Al-Kurdi
- Prof. Dr. Khaled Mohamed Abdel-Fattah Abu Shaira
- Dr. Badir Mohamed
- Dr. Abdulameer Abbas Al-khamees Ali
- Dr. Nawal Hussein Siddig
- Dr. Hussein Hamed Mahmoued Omer
- Dr. Fatima Muflih Murshid Al-Abdalat



Publication Date: 05-10-2023 ISSN: 2706-6495

Table of Content:

No	Paper title	Author Name	Country	Field	Page No
1	An Analysis of Impact Extent of Cybersecurity on Confidence in Securities Market	Sumayah Saed S. Alsahafi	Saudi Arabia	Law	5-55
2	Risk and Return of NFT, Metaverse, Cryptocurrency, and NFT's Relation with IP	Author: Bodour Idris Radwan , Co-author: Dr. Mohammed Binkhamis	Saudi Arabia	Finance	56-74
3	Detection of Pneumonia from Chest X-ray Images Using Transfer Learning and Ensemble Learning	Bahatheq Tariq Ahmed S, Jayanth Balasubramanian, Koh Shang Hui	Singapore	Computer Science	75-89
4	Fractional partial Differential Equations for Laplace transformation Caputo- Fabrizio and Volterra integration	Dr. Mariam ALmahdi Mohammed Mulla	Saudi Arabia	Mathematics	90-109
5	Psychological Stress and its Relationship to Achievement Motivation among Middle School Teachers in Palestinian Schools in Qatar in Light of Corona Crisis	Dr. Dunia Rajeh Moqpil, Professor. Mohamed Jarraya	Qatar	Sport and Physical Education	110-140
6	Ensuring Environmental Safety through Sustainable Food Safety	Aida Esaa Nasser, Khalid Abdulla Ghloom	United Arab Emirates	Food safety	141-155



An Analysis of Impact Extent of Cybersecurity on Confidence in Securities Market

By: Sumayah Saed S. Alsahafi

PhD Candidate at the University of Manchester, Saudi Arabia

Email: sumayah.sahafi@gmail.com

Abstract

Risk and opportunity more often can be seen as two sides of the same coin, for which modern technology is a fantastic illustration. This dichotomy generates prospective market disruptions and a variety of future opportunities. The history of cyberattacks is thought to have started during the cold war. This dissertation investigates cybersecurity control to maintain investors' trust in the securities market. A primary cause for the loss or decline in value of multiple financial markets was the lack of cyber-regulation in the financial sector.

Does regulation offer the best means of preserving investors' faith in securities? Is there a plan to replace it? The data demonstrates that the dangers associated with cybersecurity cause investors to lose faith in markets, resulting in considerable financial consequences. The study suggests that understanding the interrelationships with cybersecurity is crucial to maintaining the efficiency of the financial markets and keeping pace with their continuous and rapid evolution.

The dissertation also highlights claims that regulations, particularly the disclosure approach, are evaluated to determine their effectiveness in the market. Although the national regime can be successful within its region, financial markets are known to be interconnected internationally and impact each other.

Keywords: Cybersecurity, Cold War, Technology, Cyberattacks, Investors, Securities Market, Financial Markets, Regulation, Confidence, Risk, Protection, Disclosure.



1. Introduction

1.1. Research background

Demonstrating how cybersecurity and the financial markets first came together is useful to set the scene and underline its importance for this study. Therefore, we first consider the history of cybersecurity in the financial markets and then review the concepts of cybersecurity as it applies to financial markets and their importance in boosting public trust in the sector.

1.1.1. The history of cybersecurity in financial markets

The Cold War's race in science and technology led to the development of the Internet. After World War II, tensions between the United States and the Soviet Union soon increased. The 1957 launch of the Sputnik spacecraft by the Soviet Union alarmed Americans. This launch altered how the world saw the United States as a technological superpower, making the American people feel vulnerable, and raised the Soviet Union's symbolic stature. As a result, the United States government changed its approach to focus more on technology and research in response to its perceived deficit as the prospect of nuclear war hung over the nation.¹

As far as it has been known, the notion of the Internet as a self-governing cyberspace, Goldsmith and Wu argue, is now largely uprooted.² The unstoppable juggernaut that will overrun the old and outdated determinants of human governance and displace the role of territorial government has not materialised.³ Instead, something akin to a technological version of the 'cold war'' is now in danger of emerging. The dream of a self-governed global network now looks more like a collection of nation-state networks struggling with the threat of the unchecked evils of anarchy. Users must now look forward to life in the 'bordered' Internet.⁴

The crucial point is that "people may hardly expect to be absolved of conformity with the law of those countries".⁵ This is especially true if they seek to conduct business in, travel to live in, or use the infrastructure of other countries. In essence, the Internet does not maintain global cyber laws wherever it is used. On the other hand, financial markets must abide by the local regulations of

² Jack Goldsmith, 'Who Controls The Internet? Illusions Of A Borderless World' (2007) 23 Strategic Direction. ³ Goldsmith (n 2).

- ⁴ Ibid.
- ⁵ Ibid.

¹ Michael Gervais, 'Cyber Attacks and The Laws Of War' (2012) Journal of Law & Cyber Warfare 1.



where they conduct business. This suggests that local rules may be utilised to control the effects of international Internet activity.⁶

The extent of business-government cooperation has significantly increased since 1998, despite its gradual and fragmentary progress. The financial sector was the first core infrastructure area to establish such a foundation for partnerships with governments. Integrating new information technology led to efficiency improvements, which slowed the process as worries about increased vulnerability were overtaken by an interest in efficiency gains.⁷

Following these worries, financial infrastructures have become a notable target of cyber threats that have increased in sophistication and intensity. Example events included a significant North Korean offensive against the financial transaction messaging network and an impactful Iranian distributed denial-of-service (DDoS) assault.⁸ These attacks may have occurred because (i) many of the products in this sector are now digital rather than based on paper money or physical objects, and (ii) the financial industry is very integrated, and numerous businesses rely on the same technologies to perform crucial tasks, such as payments clearing and settlements.⁹

According to previous studies, breached markets experience reduced customer satisfaction and increased negative word of mouth. Although increasing shareholder value is a top priority for markets, a dearth of research exists on the impact of consumer data breaches on corporate valuations. According to Kashmiri et al., disclosing a significant investors' data breach in one US market is likely to raise investors' expectations of subsequent data breaches in other markets, leading to an interindustry contagion effect.¹⁰ However, results are inconsistent, despite a solid theoretical foundation for hypothesising a negative market response to the news of viral assaults and security breaches.¹¹

¹¹ Ali Alper Yayla and Qing Hu, 'The Impact Of Information Security Events On The Stock Value Of Firms: The Effect Of Contingency Factors' (2011) 26 Journal of Information Technology.

⁶ Ibid.

⁷ Sean Atkins and Chappell Lawson, 'Cooperation Amidst Competition: Cybersecurity Partnership In The US Financial Services Sector' (2021) 7 Journal of Cybersecurity.

⁸ Lawrence A. Gordon and others, 'Increasing Cybersecurity Investments In Private Sector Firms' (2015) Journal of Cybersecurity.

⁹ Gordon and others (n 8).

¹⁰ Saim Kashmiri, Cameron Duncan Nicol and Liwu Hsu, 'Birds Of A Feather: Intra-Industry Spillover Of The Target Customer Data Breach And The Shielding Role Of IT, Marketing, And CSR' (2016) 45 Journal of the Academy of Marketing Science.



Moreover, industry assessments indicate that markets have minimally focused on cybersecurity investments during the previous ten years. The difficulty in demonstrating the value of securities infrastructure investments appears to be the more significant barrier to obtaining adequate funding for cybersecurity needs.¹² To make effective information security investment decisions, develop an effective security management strategy, and create related policies,¹³ determining the actual cost of potential security incidents, such as virus attacks and security breaches from internal and external sources, is necessary.¹⁴

However, the cost analyses of these incidents are frequently disregarded by many markets. For example, 32% of respondents to the 2004 e-Crime Watch Survey reported not keeping track of financial losses caused by electronic or related crimes.¹⁵ A possible cause of this lack of reporting is how difficult it is to measure the cost-benefit ratios of cybersecurity efforts. Contributors to this issue include the scarcity of precise measures and efficient tools for economic and financial analysis.¹⁶

Although numerous media and trade publications exist regarding the estimated physical cost of computer virus assaults and security breaches, most of the statistics presented are rarely empirically tested for accuracy and dependability. In addition, data collection faces considerable obstacles in cybersecurity research. First, data is required to detect a security event, and it is estimated that only one-tenth of computer attacks are discovered.¹⁷ Second, challenges exist in reporting the discovered attacks. For example, of the respondents to the Crime Scene Investigation and Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey conducted in 2004, 48% acknowledged they did not disclose all instances of computer intrusion incidents, with only 20% reporting to law enforcement organisations, and 16% to internal corporate legal

¹² Hasan Cavusoglu, Huseyin Cavusoglu and Srinivasan Raghunathan, 'Economics of IT Security Management: Four Improvements To Current Security Practices' (2004) 14 Communications of the Association for Information Systems.

¹³ Anat Hovav and John D'Arcy, 'The Impact of Denial-Of-Service Attack Announcements on the Market Value Of Firms' (2003) 6 Risk Management and Insurance Review.

¹⁴ Yayla and Hu (n 11).

¹⁵ Josh McNutt, 'Analysis of the US-CERT DAC' (2004) Carnegie-Mellon University Pittsburgh Pa Software Engineering Inst.

¹⁶ Yayla and Hu (n 11).

¹⁷ Seymour Bosworth and Michel E. Kabay (eds) 'Computer security handbook' (John Wiley & Sons, 2002).



councils.¹⁸ This low reporting rate exacerbates the estimate that only 10% to 20% of all cyberrelated attack occurrences are discovered.¹⁹ A primary justification for not disclosing is the concern that unfavourable publicity may significantly affect the organisation's stock price.²⁰

After an attack, many compromised organisations spent millions of dollars bolstering security measures and tightening security controls. However, more than 20% of the compromised markets still experienced significant losses in income, clientele, and business opportunities. As a result of the potential impact on business value and operations, cybersecurity is swiftly increasing as a priority by corporate governance and executive leadership. For instance, 88% of CEOs in the United States are concerned that cyberattacks could obstruct the growth of their businesses. Similarly, investors are now asking for more information on data breaches, cyber-security concerns, and how markets manage these risks.²¹

Responding to these increased concerns, in May 2011 the Securities and Exchange Commission (SEC) hosted a roundtable meeting to explore the cybersecurity landscape and disclosure problems to address the growing cyber risks. Following this, the SEC's Division of Corporation Finance released disclosure recommendations on cybersecurity in October 2011²² to help businesses decide when to disclose cybersecurity risks.

In response to multiple accounting disasters at companies like Enron and WorldCom, the Sarbanes-Oxley Act (SOX) of 2002 was passed. Stockholders of these companies lost their jobs and a significant portion of their asset value, including entire retirement savings for many. The SOX Act is not a deterrent to financial and accounting crimes but supports maintaining investors' faith in the stock market, although it is not flawless.²³

¹⁸ Yayla and Hu (n 11).

¹⁹ Bosworth and Kabay (n 17).

²⁰ Sotirios Pirounias, Dimitrios Mermigas and Constantinos Patsakis, 'the Relation between Information Security Events and Firm Market Value, Empirical Evidence on Recent Disclosures: An Extension of the GLZ Study' (2014) 19 Journal of Information Security and Applications.

²¹ He Li, Won Gyun No and Tawei Wang, 'SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors' (2018) 30 International Journal of Accounting Information Systems.
²² Ibid.

²³ Dave Chatterjee, 'Should Executives Go To Jail Over Cybersecurity Breaches?' (2019) 29 Journal of Organizational Computing and Electronic Commerce.



National efforts are emerging to organise cybersecurity within the financial markets.²⁴ However, the global, interrelated structure of financial markets makes it challenging for governments to agree on international legislation or specific strategies to prevent attacks that could distribute impact between them.

1.1.2. The concept of cybersecurity

According to the SEC, cybersecurity is "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorised access".²⁵ However, the SEC does not define a cyberattack. The American Department of Defense makes three distinctions between various computer network operations: (i) The term computer network defence (CND) refers to measures taken "to protect, monitor, analyse, detect and respond to unauthorised activity within Department of Defense information systems and computer networks", (ii) computer network attacks (CNA) are defined as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves", and (iii) computer network exploitations (CNE) are defined as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks".²⁶ Legal studies typically ignore military views of CND or CNE in favour of concentrating on CNA, commonly referred to as cyberattacks.²⁷

To carry out a successful cyberattack, the attacker must have access to the target's computer or network, either remotely (through the Internet) or locally (through a thumb drive, for example). This access is necessary to exploit a vulnerability, such as modified software or hardware, and deliver a 'payload', which is typically software that, once installed on the target computer, performs a variety of nefarious tasks, such as "reproducing and retransmitting itself, destroying files on the system, or altering files". People within a targeted organisation remain the weakest

²⁷ Ibid.

²⁴ Ibid.

 ²⁵ Matthew F. Ferraro, 'Groundbreaking' Or Broken?: An Analysis Of SEC Cyber-Security Disclosure Guidance, Its Effectiveness, And Implications' (2013) SSRN Electronic Journal.
 ²⁶ Ferraro (n 25).



point in computer network security as unsuspecting computer users who download harmful software, misplace hardware, or carelessly publish confidential information online.²⁸

However, modern definitions of cyberattacks exclude or ignore that they can have severe economic consequences just as their kinetic counterparts, as illustrated in the following example. A fighter jet from state A flies into the airspace of state B and launches a bombardment on a farm and its crop field, utterly and irreparably destroying both. The physical damage is evident, as can be seen by the farm's devastation and crops burned. The financial loss is quantifiable, such as in this example, as having a replacement cost of \$500,000. Here, it is clear that a kinetic weapon (i.e., the fighter jet's attached bombs) had kinetic consequences (physical destruction of a farm and crops). Now, consider a second hypothetical non-kinetic attack. An export credit agency (ECA) intrudes into the computer networks of state B's central stock exchange and manipulates and deletes information worth \$500,000. Because no kinetic weapons were employed in this scenario, the ECAs may not be taken as seriously as the aircraft strike.²⁹

From an impact perspective, damage worth \$500k was caused in the first and second scenarios. According to some experts, such meddling with a state's economic health is "equivalent to an armed attack" from this impact-based perspective.³⁰ The second situation is likely to be considered less severe than the use of physical force. However, the first scenario would be categorised as using force, which is forbidden under international law. The different circumstance surrounding the act of the attack, for example, the use of military weapons following an intrusion into the sovereign airspace of state B, is what matters when classifying these events instead of the effects of the impact of the event, which appears to be the key consideration under international law regarding the use of force. In the age of cyber warfare, such difference may no longer be necessary, especially given the immense economic damage that a cyberattack can inflict.³¹

1.1.3. The value of cybersecurity to support confidence

As mentioned above, executives of organisations are gradually elevating cybersecurity to a key priority because no market is immune to cybersecurity risks. Following legislative developments,

²⁸ Ibid.

²⁹ Ido Kilovaty, 'Rethinking the prohibition on the use of force in the light of economic cyber warfare: towards a broader scope of Article 2 (4) of the UN Charter', (2014) JL & Cyber Warfare 4: 210.

³⁰ Kilovaty (n 29).

³¹ Ibid.



cybersecurity is essential across all industries and even more important in the financial sector to increase protection for investors. Cybercrimes will continue to raise the risk of hacker attacks as digital data in the financial sector expands.³²

This cybersecurity challenge is a primary concern for regulators and is gaining more attention from global organisations, such as the Financial Stability Board (FSB), Basel Committee and SEC. Cybersecurity is considered one of the largest concerns facing the financial sector, especially as process centralisation and digitisation develop along with financial institutions' internal concentration on the risks. Similarly, for new financial start-ups, these data-intensive markets frequently have a limited understanding or perception of security needs because they operate within a digital environment with a wealth of data. As a result, cybersecurity should be a top priority for these markets.³³

Without the currently enabled technology, the financial markets of today are worthless. A market plan can benefit more from technology. Data can be stored, retrieved, analysed, reported, and redistributed without difficulty. Projecting annual growth and long-term goals are frequent practises among financial institutions. Technology serves as a tool to enhance operations and visibility for achieving these goals.³⁴ However, cybersecurity technologies exist to prevent all attacks and to consolidate the confidence and protection for the investors.

1.2. Aims of the research

The assessment above highlights the value of cybersecurity for financial securities and the effects cyberattacks have on financial markets, as well as how crucial strong cyber laws and investment policies are to the security and stability of financial markets.

This research evaluates how successfully investor trust has been safeguarded by regulatory reforms connected to cybersecurity. Examined are the most recent revisions to general frameworks for financial cybersecurity and cyber threats that harm the securities markets. Also, this study demonstrates if someone or some organisation is willing to take responsibility for an accused

³² Jennifer Callen-Naviglia and Jason James, 'FinTech, RegTech and the Importance of Cybersecurity' (2018) Issues In Information Systems.

³³ Douglas W. Arner, Janos Barberis, and Ross P. Buckey, 'FinTech, RegTech, and the reconceptualization of financial regulation', (2016) Nw. J. Int'l L. & Bus.37 : 371.

³⁴ Gurdip Kaur, Ziba Habibi Lashkari and Arash Habibi Lashkari, *Understanding Cybersecurity Management In Fintech*, (Cham: Springer, 2021).



attack and stand up for the rights of the investors. Furthermore, the sector's exposure to these cyber-related risks can increase our understanding of the problem. Alternative strategies and regulation as a single financial sector response to cyber gaps are also discussed.

To protect investors, this dissertation demonstrates how disclosure alters the way financial markets operate. Also, an assessment of these disclosures is made to determine if the current framework varies in its application basis. The effects of disclosure are illustrated through specific cases that help identify the accountable party when disclosures are made incorrectly. These results suggest discloser benefits as an acceptable strategy to safeguard investors and markets.

The findings provide the basis for a study on cybersecurity disclosure in financial securities. With respect to cyberspace, this study evaluates how well regulation curbs risk-taking in financial institutions and suggests that regulations should consider these issues to ensure the effective expansion of cybersecurity operations. Evaluating if regulation is the best strategy to preserve the trust of investors in securities is a foundational aspect of this investigation, and these results can influence the field of financial policy and regulation.

1.3. Methodology

This dissertation uses a doctrinal approach to demonstrate how cybersecurity and financial securities can be combined to gain increased trust and protection of investors through an exposition of the rules governing cybersecurity in financial markets, analyses of the regulations, an explanation of problematic regions, and a potential prediction of future developments. A careful review of primary and secondary legal resources enables an in-depth investigation of the connections between certain variables and cybersecurity legal loopholes in the financial sector. Using this doctrinal perspective supports an enhanced understanding of the implications of this issue for financial markets.

Failure of cybersecurity in financial markets can create financial system disruptions at national and international levels and result in significant losses for investors because they are the most atrisk group. A study of expanding cybersecurity in the financial sector offers crucial information for maintaining the financial system's stability. A lack of international consensus that prevents all nations from reaching an agreement on cybersecurity challenges also motivates this study, which considers if the best approach to preventing attacks is to increase broad investment in cybersecurity so these incidents can be handled at an international scale.



1.4. Dissertation structure

Chapter 2 examines the cybersecurity concerns brought on by assaults on financial securities. This study considers some cases that significantly impacted financial markets because it is primarily concerned with analysing regulatory trends. This chapter also demonstrates if there is someone to blame for these attacks to address the protection of investors' rights. Next, this chapter considers how these dangers affect financial markets and argues how regulation can be the sole solution for these impacts. To assess the advantages and disadvantages of the pertinent legislation, the characteristics of these interactions are reviewed.

Chapter 3 evaluates disclosure regulation as the primary regulatory tactic leveraged by many rules to report the state of cybersecurity within the financial sector. The background of disclosure facilitates comprehension of the approach's beginning and significance. Due to this, the conclusions from other studies offer a useful tool for evaluating these strategies. Also, various viewpoints are asserted as presenting a more accurate picture of disclosure. The SEC-recommended disclosure process is demonstrated as being followed. The example scenario is presented where disclosure violates Rule 10b-5, resulting in the identification of the accuser, which is pertinent to the context of this study. Chapter 3 concludes the argument by the avails of disclosure to protect investors and markets.

Chapter 4 concludes with a summary of the thesis objectives and research question and emphasises the significance and applicability of the study. Also, a summary of the debate of how the research leads to some advances is discussed, followed by an outline of the significance of the findings for financial market cybersecurity efforts. Finally, this chapter highlights areas that could benefit from additional study to advance knowledge of cyber processes in financial markets and the regulatory consequences.

2. Analysis of the confidence state in financial securities

Highlighting the importance of cybersecurity, as discussed in the previous chapter, requires an illustration of the risks in the financial sector, which facilitates an understanding of the ways in which to gain investors' confidence. Demonstrating the risks as we will do, provides a basis for determining who is responsible for risk-taking. This chapter further examines a wide range of influences of those risks on investors' confidence. The chapter concludes with an outline of the flaws of the strategy of regulation as the sole solution to preventing risk-taking behaviours.



2.1. Exposing the harmful risks in financial securities

Technology today is a great example of how risk and opportunity are progressively becoming two sides of the same coin. Technology is the source of many opportunities, as well as potential disruptions.³⁵ Risk is, in general, the likelihood that anything may go wrong. It concerns the uncertainty in different spheres of a person's daily life. For instance, a businessperson may view declining pricing as a risk to their company's revenue if they are uncertain whether the pricing will recover. Even more so than with trends such as that in the example, the risk of incurring the negative effects of a single or sequence of accidents most greatly affects investors' confidence.³⁶

Financial institutions are primary targets of cyberattacks today because they largely run online. Sixty per cent of financial organisations employ cloud services, the majority of which are private clouds. In that context, there is an urgent need for the threat landscape to be explored, given how sophisticated cyber threats are becoming and the increased diversity and intensity of attacks. Cyber dangers take the form of security incidents that jeopardise the confidentiality, integrity or accessibility of data.³⁷

To explore risks in this field, most studies use data on cyberattacks obtained directly from the market. However, managers can be strongly motivated to keep knowledge about cyberattacks a secret, particularly if the attack's occurrence and the extent of the harm it caused were unforeseen. Managers have been found to only reveal information about less damaging attacks, while keeping investors in the dark about any that were worse. In particular, if investors are unsure whether a company has information security issues, the management will withhold negative information unless it falls below a certain threshold.³⁸ Such behaviour can be counterproductive though since, often, while the market's response to disclosures of attacks is modest, the leakage of information on attacks previously covered up provokes an adverse and considerable response.³⁹

Accordingly, there is evidence that businesses, in general, are paying closer attention to cyberattacks. As of 29 June 2014, 1517 companies listed on the New York Stock Exchange

³⁵ Maricela Ramírez and others, 'The Disclosures of Information on Cybersecurity in Listed Companies in Latin America: Proposal for a Cybersecurity Disclosure Index' (2022) 14 Sustainability.

³⁶ Kaur, Lashkari and Lashkari (n 34).

³⁷ Kaur, Lashkari and Lashkari (n 34).

³⁸ Ibid.

³⁹ Eli Amir, Shai Levi and Tsafrir Livne, 'Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets' (2018) 23 Review of Accounting Studies.



(NYSE) or National Association of Securities Dealers Automated Quotations (NASDAQ) included cybersecurity, hacking, cyberattacks or data breaches as potential business risks in their securities filings.⁴⁰ This followed a trend of increase compared to the previous two years (2013, 1288; 2012, 879). Against the background of heightened risk, the boards of publicly traded companies have adopted different strategies for their cybersecurity monitoring, with some utilising the whole board, others the audit committee and others a technology committee, while some are yet to produce active monitoring plans. SEC Commissioner Luis Aguilar noted a discrepancy between the degree of risk of security breaches and the measures boards have taken to manage that risk.⁴¹ As a result, the implication is that many markets are still ill-equipped to handle cyber threats.⁴²

Threat actors come in many forms, including professional cybercriminals, amateur hackers and rival nation-state security services. Foreign governments with the means and motivation to undermine or abuse the financial system are the most worrisome actors from a systemic standpoint. Some, such as North Korea, wish to take advantage of the system without thinking about the long-term effects. Others, such as Iran, wish to undermine the financial services in an effort to compete with the United States and its allies on a geostrategic level, while others still, such as Russia, aim to put systems at risk to act as a deterrent.⁴³

The costs of these attacks may be high. To provide examples, a data breach of Target Corporation in 2013 with an estimated cost of at least \$162 million affected almost 40 million consumers.⁴⁴ Verizon Communications, meanwhile, when attempting to acquire Yahoo!, reduced its offer price by \$350 million after Yahoo! disclosed it had fallen victim to a 2014 cyberattack.⁴⁵ More recently, private financial data of roughly 143 million Americans was leaked in a breach at Equifax. Over 240 class action lawsuits are being defended by the company as a result, and \$87.5 million has

⁴⁰ Danny Yadron, 'Boards Race to Fortify Cybersecurity' (2014) The Wall Street Journal.

⁴¹ Yadron (n 40).

⁴² Julia L. Higgs and others, 'The Relationship between Board-Level Technology Committees and Reported Security Breaches' (2016) 30 Journal of Information Systems.

⁴³ Atkins and Lawson (n 7).

⁴⁴ Brian Prince, 'Shifting Priorities: How Enterprises are Safeguarding against Cybersecurity Threats' (2015) 196 Forbes 119–124.

⁴⁵ Henk Berkman and others, 'Cybersecurity Awareness and Market Valuations' (2018) 37 Journal of Accounting and Public Policy.



already been spent on legal fees.⁴⁶ Cyberattacks such as these have compromised incredibly sensitive information, intellectual property and personal financial information, among others. Global economic losses from cybercrime are estimated to exceed \$450 billion.⁴⁷ Considering this, it is clear to see how breaches have a detrimental effect on market valuations and investor protection.⁴⁸

2.2. Who should be accused of failing to protect against risks?

An organisation should ideally be committed to protecting sensitive data, and accordingly, take every reasonable precaution and measure. The organisational representative can then, and only then, effectively address the concern that stakeholders are likely to have following a successful attack: "What did this institution do to prepare?" Such a representative should not be punished for the cyberattack if every attempt was made to prevent data breaches.⁴⁹

Looking higher up the chain of command, it can be challenging to hold directors accountable for institution losses, as highlighted by the renowned decision made by the Delaware Court of Chancery in the Caremark International Inc. Derivative Litigation. In cases when a director's choice results in a loss, culpability is often assessed according to the director-protective business judgement rule, providing the decision was the result of a process that was either consciously evaluated in good faith or was otherwise sensible. Rather than subjecting directors to judges' or jurors' second-guessing, which may harm investors' interests, to allow for an impartial assessment of the choice then an investigation into the decision-making process is advisable. As such, the business judgement rule is process-oriented and underpinned by a great respect for all choices made by the board in good faith.⁵⁰

When employees at Caremark caused losses by breaking federal laws, the court determined that "plaintiffs would have to show either (i) that the directors knew or (ii) should have known that

⁴⁹ Chatterjee (n 23).

⁴⁶ Char Sample and others 'Culture + Cyber: Exploring the Relationship' In Advances in Human Factors in Cybersecurity (2017), 185–196.

⁴⁷ Higgs and others (n 42).

⁴⁸ Lawrence A. Gordon, Martin P. Loeb and Tashfeen Sohail, 'Market Value of Voluntary Disclosures Concerning Information Security' (2010) 34 MIS Quarterly; Sangmi Chai, Minkyun Kim and H. Raghav Rao, 'Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior' (2011) 50 Decision Support Systems.

⁵⁰ Edward A. Morse, Vasant Raval and John R. Wingender Jr. 'SEC Cybersecurity Guidelines: Insights into the Utility of Risk Factor Disclosures for Investors' (2017) 73 The Business Lawyer 1–34.



violations of the law were occurring and, in either event, (iii) that the directors did not take any steps in a good faith effort to prevent or remedy that situation, and (iv) that such failure proximally resulted in the losses complained of". The court stated that this standard would be difficult to satisfy because it would effectively call for a lack of good faith in the performance of supervisory obligations.⁵¹

Accordingly, board decisions to use staff or technology to address cybersecurity concerns are likely to be shielded from liability claims in shareholder derivative lawsuits. Even if the market's cybersecurity precautions prove unsuccessful, the process-oriented business judgement rule seems to offer substantial protection for real board decisions. In the same way, allegations that directors failed to keep an eye on or exercise oversight over cybersecurity concerns are unlikely to prevail if the directors can show that they acted in good faith.⁵²

In other cases, authorised personnel can pose serious cyber threats by misusing their authority and privileges. In further cases still, employees can cause potential damage unintentionally. For example, an employee can be a victim of a phishing attack if they click a malicious link that covertly downloads malware on their workstation/computer to create a backdoor.⁵³

A high-performance security culture that encompasses the three core characteristics of dedication, preparation and discipline must have the support of the top management if it is to succeed.⁵⁴ The senior leadership is crucial for establishing security mechanisms that provide confidence, for requiring security audits and drills, demanding sufficient resources, rallying organisation-wide support, monitoring the performance constantly, enforcing security policies and so on.⁵⁵ They must take a hands-on approach, with great attention and effort if they are to comprehend the organisational weaknesses and what it will take to overcome the obstacles.⁵⁶

It is bad practice to assign responsibility for cybersecurity to a group of security experts and then hold them accountable for failure.

⁵¹ Morse, Raval and Wingender (n 50).

⁵² Ibid.

⁵⁶ Chatterjee (n 23).

⁵³ Kaur, Lashkari and Lashkari (n 34).

⁵⁴ P. K. Chatterjee, 'City Hosts a Highly-Heralded Cyber Security Event' (2018) Free Press Journal.

⁵⁵ Salah Kabanda, Maureen Tanner and Cameron Kent, 'Exploring SME Cybersecurity Practices in Developing Countries' (2018) 28 Journal of Organizational Computing and Electronic Commerce.



This is a symbolic check-the-box strategy that is unlikely to yield real outcomes. Every organisational member must take joint ownership, duty and accountability for the security preparation, which must be led by top leaders to protect investors.⁵⁷

2.3. Growing influences on risk-taking or risk-averse behaviours

A cyberattack often provokes reactions from investors, with a number of studies having demonstrated a correlation between negative cybersecurity events (e.g. when software vulnerability notifications are made,⁵⁸ announcements of IT products having viruses⁵⁹ or reports of cybersecurity breaches⁶⁰) and low stock prices.

Looking in further detail, according to Campbell et al. in their 2003 study, there is a considerable negative market reaction to breaches involving violations of confidentiality but no discernible market response to other breaches. The authors concluded that as cybersecurity safeguards a variety of market assets, the economic repercussions of a security breach depend on the type and worth of the underlying assets affected.⁶¹

It has been demonstrated that breaches concerning major e-businesses in charge of sensitive data, such as Amazon, eBay, Yahoo, First Data Corporation and JP Morgan Chase, are likely to be perceived as having major economic consequences. Due to the massive volumes of sensitive data that these companies collect, keep and transport, any news of a cybercrime involving them is likely to cause a big, negative, anomalous return on their stock prices.⁶²

In addition, the nature of the event determines how a cybersecurity incident or breach provokes a market reaction.⁶³ Wang et al. demonstrated that the market's reaction to a security breach may

62 Ibid.

⁶³ Yayla and Hu (n 11).

⁵⁷ Ibid.

⁵⁸ Rahul Telang and Sunil Wattal, 'An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Prices' (2007) 33 IEEE Transactions on Software Engineering.

⁵⁹ Anat Hovav and John D'Arcy, 'Capital Market Reaction to Defective IT Products: The Case of Computer Viruses' (2005) 24 Computers & Security.

⁶⁰ Henk Berkman and others, 'Cybersecurity Risk Mitigation, Private Information Leakage and Earnings Announcements' (SSRN Electronic Journal, 1st December 2018) < https://www.researchgate.net/profile/Jonathan-

Jona/publication/325752038_Cybersecurity_Awareness_and_the_Cost_of_Liquidity/links/5d726f0b92851cac db23ff46/Cybersecurity-Awareness-and-the-Cost-of-Liquidity.pdf > accessed; Amir, Levi and Livne (n 39).

⁶¹ Edward A. Morse, Vasant Raval and John R. Wingender, 'Market Price Effects of Data Security Breaches' (2011) 20 Information Security Journal: A Global Perspective.



depend on the specificity of the information provided—when the breach report contains highly specific details regarding the breach, the market reacts more negatively.⁶⁴

Through case study investigations, Andoh-Baidoo, Amoako-Gyampah and Osei-Bryson examined the changes to the market values of companies whose systems had been compromised, to gauge the impact of different Internet security breaches.⁶⁵ An announcement regarding a company's Internet security vulnerability in a significant American newspaper was their definition of an event. The three-day event window they used for their analysis comprised the day before the event to the day after the event. Their sample of 110 incidents, which was ultimately reduced to 41 events, was sourced from reportage in the Wall Street Journal, New York Times, Financial Times, Washington Post and USA Today, concerning breaches between 1997 and 2003. On average, the companies in their survey saw a 3.18 per cent decline in market value. Of the 41 firms, all reported abnormally low returns; for 27 firms, the returns were negative, while 14 reported zero or positive returns during that time.⁶⁶

From another perspective, Martin et al. considered the impact of a data breach on peer organisations as dependent on the breach's severity. While low-severity data breaches have a detrimental impact on competing firms' performance, higher-severity data breaches can be beneficial for them as clients of the breached company are then inclined to switch to a rival company due to the circumstances. According to Kashmiri et al., a peer firm's ability to prevent a similar data breach through its IT, its commitment to corporate social responsibility and its marketing acumen in the wake of the breach of the unlucky firm all have a moderating effect on the impacts of the breach on that peer firm.⁶⁷ Cyberattacks and security breaches may hurt peer companies, but at the same time, they will increase the market value of information security service providers such as those offering Internet security software and services and IT consulting firms.⁶⁸ An organisation can be impacted by a cyberattack in a variety of ways, and these effects will change based on the type and gravity of the attack: (i) Above the surface as tangible costs: technical

⁶⁴ Berkman and others (n 60).

⁶⁵ Francis Kofi Andoh-Baidoo, Kwasi Amoako-Gyampah and Kweku-Muata Osei-Bryson, 'How Internet Security Breaches Harm Market Value' (2010) 8 IEEE Security & Privacy Magazine.

⁶⁶ Morse, Raval and Wingender (n 61).

⁶⁷ Berkman and others (n 60).

⁶⁸ Michael L. Ettredge and Vernon J. Richardson, 'Information Transfer Among Internet Firms: The Case of Hacker Attacks' (2003) 17 Journal of Information Systems.



investigation, customer breach notification, post-breach customer protection, regulatory compliance, public relations and cybersecurity improvements. The intangible costs might have a long-term impact on the firm's anticipated future cash flows, whereas the majority of tangible expenses are immediate or short-term; (ii) Beneath the surface as hidden or intangible costs: insurance premium increases, increased cost to raise debt, lost value of customer relationships, value of lost contract revenue, attorney fees and litigation, devaluation of trade name and loss of intellectual property. The Washington Post claims that there was an increase in cybersecurity breaches of over 50% between 2007 and 2008. Despite the fact that these violations affect a wide range of institutions, there is general agreement that they may be quite costly for markets: "lost current and future revenues brought on by the deterioration of a company's relationships with both its clients and its business partners; potential legal repercussions related to violations".⁶⁹

Some recent studies point to a decrease in the average cost of cybersecurity breaches in recent years. That is, there appears to be a movement in investors' perspectives toward considering cybersecurity breaches as a corporate 'nuisance' or simply another regular operating cost, as opposed to posing a potentially major financial danger to the existence of markets.⁷⁰

Other potential explanations for the waning effects of security breaches, according to Gordon et al., include successful recovery plans or clients who are more steadfastly willing to continue doing business with the afflicted organisations. Given the cumulative frequency of these instances over the past few years, customers now perceive security breaches as less serious than in the past. Hence, customers might now be more inclined to deal with enterprises that have experienced a breach due to the relatively routine occurrences of such breaches, in contrast to the beginning of the Internet age, when hacker assaults constituted a new and frightening phenomenon.⁷¹

A serious issue has been created lately by an apparent shift in investors' perspectives on data security incidents. Corporate executives have taken cues from investors to keep their firms' information security investments at the current level, or at least not raise them significantly, with modern investors viewing security breaches as more like a nuisance than as a potentially serious

⁶⁹ Lawrence A. Gordon, Martin P. Loeb and Lei Zhou, 'The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?' (2011) 19 Journal of Computer Security.

⁷⁰ Ibid.

⁷¹ Oliver Hinz and others, 'The Influence of Data Theft on the Share Prices and Systematic Risk of Consumer Electronics Companies' (2015) 52 Information & Management.



economic threat to the survival of firms. Yet, this opens up the risk that a big unanticipated breach, or the famous "black swan", has the potential to endanger a company's viability.⁷²

Hovav and D'Arcy investigated how security breaches such as viruses, worms and denial-ofservice. Yet, the researchers concluded that the relative impact of each type of breach versus the others was uncertain.⁷³ Telang and Wattel, meanwhile, in a study specifically on software vendors' disclosures of vulnerabilities, discovered that each time a vulnerability was exposed, businesses experienced a market value loss of about 0.6 per cent, or roughly \$0.86 billion, for each market.⁷⁴ Some security breach research has documented how the stock market reacts negatively and significantly when there has been a security breach. Garg et al., for instance, charted "cybersecurity incidents" that occurred between 1996 and 2002. The occurrences include denial-of-service attacks, computer viruses and the theft of confidential information, in addition to situations where customer data were exposed. They discovered that for the enterprises concerned, the typical abnormal return was 5.3% over the three days that followed the occurrence.⁷⁵ Similar results were found by Cavusoglu et al., who discovered anomalous returns over a two-day timeframe of 2.1 per cent for 66 incidents between 1996 and 2001, where the markets reacted to "malicious attempts to interfere with a company's activity and its information". Both assaults on proprietary data and its integrity, and compromises of personal information, were included in the researchers' classification.76

Elsewhere in the literature, Ko and Dorantes compared the one-year financial performance of companies that faced cybersecurity breaches between 1997 and 2003 to similar companies without breaches using a matched-firm analysis. They investigated 19 businesses whose data were accessed improperly. Ko and Dorantes showed that while the performance of the security-breached enterprises was not significantly affected the following year, they tended to lag behind those that had not experienced a breach.

⁷⁶ Kevin M. Gatzlaff and Kathleen A. McCullough, 'The Effect of Data Breaches on Shareholder Wealth' (2010) 13 Risk Management and Insurance Review.

⁷² Gordon, Loeb and Zhou (n 69).

⁷³ Hovav and D'Arcy (n 59).

⁷⁴ Sanjay Goel and Hany A. Shawky, 'Estimating the Market Impact of Security Breach Announcements on Firm Values' (2009) 46 Information & Management.

⁷⁵ Ashish Garg, Jeffrey Curtis and Hilary Halper, 'The Financial Impact of IT Security Breaches: What Do Investors Think?' (2003) 12 Information Systems Security.



The results offered "partial support" to their hypothesis that organisations that experience security breaches will go on to perform worse than their counterparts.⁷⁷

The factors most likely to affect the size and direction of the stock price response to news of a security event are subject to debate among researchers. Occasionally, a company's characteristics and its performance on the stock market can be linked.⁷⁸ Hovav and D'Arcy's 2003 investigation found that a denial-of-service assault had significant negative effects for a subset of Internet-only businesses, but their overall sample showed no evident stock market reaction.⁷⁹ Similar to this, Cavusoglu et al. discovered that security breaches of online enterprises were more strongly connected to a negative stock price response than breaches of traditional firms. They also discovered that the attacks size had a moderating impact on the stock price response.⁸⁰

Some researchers have explored events' characteristics in an effort to explain the sizes and patterns of stock price reactions to news of security problems, finding that the type of breach may influence how the stock market reacts.⁸¹ Similar to this, the main finding by Campbell et al. was that the type of breach might influence the stock market reaction, with illegal data access, in particular, strongly related to an adverse stock market response.⁸² In contrast to those findings, however, Cavusoglu et al. discovered that cases of unauthorised access to data in their sample were not punished more severely than other instances of security breaches. Accordingly, they concluded that the kind of breach did not affect how the stock market reacted to the incident.⁸³

There are likely to be two potential securities market reactions to a leak of sensitive consumer data. Perhaps, as demonstrated by Cavusoglu et al. and Garg et al., the market may respond negatively to news of a breach, showing an awareness of the potential consequences of breaches.

⁷⁷ Myung Ko and Carlos Dorantes, 'The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation' (2006) 17 Journal of Information Technology Management 13–22.

⁷⁸ Gatzlaff and McCullough (n 76).

⁷⁹ Hovav and D'Arcy (n 59).

⁸⁰ Huseyin Cavusoglu, Birendra Mishra and Srinivasan Raghunathan, 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' (2004) 9 International Journal of Electronic Commerce.

⁸¹ Gatzlaff and McCullough (n 76).

⁸² Katherine Campbell and others, 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market' (2003) 11 Journal of Computer Security.

⁸³ Cavusoglu, Mishra and Raghunathan (n 80).



Alternatively, as observed by Hovav and D'Arcy and Campbell et al., there may be no significant securities market response to news of a data breach. The latter case could indicate that these occurrences have become so routine that they no longer provoke a major market reaction.⁸⁴

Strangely, not every victim of a data breach encounters the same effects on their market price. Investors in the financial services sector are keenly aware of the consequences of data security because this is where the majority of sensitive data is stored and often exchanged. Financial services is the largest industry in terms of transaction volume and frequency, implying higher risk exposures and hence bigger potential losses. Furthermore, market capitalisation losses significantly impact financial services firms.⁸⁵

Investors, who perceive breaches of employee or customer data unfavourably, especially in markets with great potential for growth, should be aware of these. A high decline in shareholder value is also often linked to a refusal by the firm affected to disclose specifics about the breach, a scenario firms should thus be wary of creating. In addition, since firms operating in larger markets are mostly shielded from a negative market-wide reaction to news of a data breach, firms operating in smaller markets appear to have most reason to fear the consequences of a breach occurring.⁸⁶

It is difficult to assess the costs incurred by catastrophic breaches. For instance, a researcher at Mizuho Investor Securities first estimated the cost of the 2014 Sony hack to have been \$1.25 billion. However, in such cases, the figures given by the firms targeted are substantially lower. Sony estimated that in the year following the incident, the cost of the investigation and corrective actions was \$35 million. Another point worth mentioning is that most enterprises in major markets have insurance to cover a portion of their cyber risk; then, the enterprise, its insurance firm and the taxpayer will all bear a roughly equal share of the operational expenses of a cyber-breach.⁸⁷

In summarising the findings from the literature presented here, the conflicting results on how cybersecurity breaches affect publicly traded companies' stock market returns are concerning for at least two reasons. First, the results of multiple surveys and anecdotal evidence repeatedly demonstrate that the costs associated with cybersecurity breaches are high, both generally and with

⁸⁴ Gatzlaff and McCullough (n 76).

⁸⁵ Morse, Raval and Wingender (n 61).

⁸⁶ Gatzlaff and McCullough (n 76).

⁸⁷ Gilles Hilary, Benjamin Segal and May H. Zhang, 'Cyber-Risk Disclosure: Who Cares?' (2016) SSRN Electronic Journal.



respect to particular types of breaches. Therefore, it appears, at least on the surface, that the contradictory findings about the effect of security breaches on stock market returns occur. Second, though this is so far missing from the literature, the costs and benefits of breaches should be compared to determine how much an organisation should spend on cybersecurity activities, such as preventing, detecting and resolving security breaches. Making judgments about investments in cybersecurity activities requires a thorough understanding of the true impacts of security breaches on the securities market returns of organisations, encompassing both the implicit and explicit costs of breaches.⁸⁸

2.4. Regulation as the sole solution for mitigating influences

At present, there are three clear barriers to regulating cybersecurity in the financial sector. First, the field of cybersecurity seems resistive to codifying the relevant laws in a thorough multilateral binding convention. Second, governments have demonstrated a strong unwillingness to contribute to the creation of international customary laws related to the cybersphere. They have been hesitant to provide explicit expressions of opinion juris on issues linked to cybersecurity, and state conduct in this field is inherently cloaked in secrecy.⁸⁹

While the first two relate to states' unwillingness to act in ways that are meaningful for the formation of new regulations, the third issue is states' actual behaviour in respect to cyber governance. To say that states have completely abandoned standard-setting would be untrue as there are mandatory or non-mandatory national cyber regulations to protect financial markets,⁹⁰ such as the General Data Protection Regulation (GDPR), Cybersecurity Disclosure Guidance by the SEC, the National Institute of Standards and Technology (NIST), the SOX, the Gramm–Leach–Bliley Act (GLBA) and the Office of the Superintendent of Financial Institutions (OSFI).

When the rise in cyber events, relating to the risks detailed in Section 2.1, caught the attention of both the state and federal governments, regulations were put in place by the State of New York in 2017 that mandate financial service businesses to create cybersecurity procedures and submit yearly certifications attesting their compliance.⁹¹ According to Fischer, in 2014, there were 56

⁸⁸ Gordon, Loeb and Zhou (n 69).

⁸⁹ Kubo Mačák, 'Is the International Law of Cyber Security in Crisis?' (2016) 8th International Conference on Cyber Conflict (CyCon), IEEE 127–139.

⁹⁰ Ibid.

⁹¹ New York 23 NYCRR 500 2017.



federal laws in the United States that dealt with cybersecurity,⁹² and that figure will now only have increased. In May 2018, the first cybersecurity law in the European Union (EU) came into force, requiring a wide range of businesses to report any breaches they encounter. Following on from this, in the EU, further cybersecurity legislation is now in the works.⁹³

When national governments' understanding of the risks of cyberattacks is promoted, their willingness to submit to internationally binding rules tends to improve. With reference to key developments in the past that were at first not well-understood, despite the dominant spacefaring governments' initial strong resistance, the domain of outer space eventually became subject to a binding legal regime. Moreover, the first worldwide nuclear safety rules were not implemented for almost three decades after the launch of the world's first nuclear power station in 1954 in Obninsk, Soviet Union (now Russia). In the interim, non-binding safety standards and criteria, the majority of which were produced by the International Atomic Energy Agency, served as guidance for governments (IAEA). Later, nuclear safety treaties unified this developing corpus of non-binding standards and made many of the pertinent requirements obligatory for all member states.⁹⁴

A number of factors have delayed the expansion of cyber financial regulation. For instance, cybersecurity capabilities are heavily influenced by the market's size and segmentation. Smaller companies have historically trailed behind large corporations. In that context, the financial sector has not yet discovered an efficient method for achieving cyber financial regulation that will not place an unfair burden on smaller markets. In addition, sustaining the progress that giant corporations have made across the system remains a key problem.⁹⁵

Moreover, though key players in different markets believe information exchange on risks and vulnerabilities to be highly beneficial, they are also compelled to work against government and industry cooperation in this area. Since market operations and reputations are tightly linked to the cyber infrastructure, knowledge of these systems and security lapses is linked to organisations' competitive advantage. Although the strength of this motivation to shirk cooperation has diminished over time as businesses have discovered that it is generally not in their best interests to

⁹² Eric A. Fischer, 'Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation' (2014).

⁹³ Berkman and others (n 60).

⁹⁴ Mačák (n 89).

⁹⁵ Atkins and Lawson (n 7).



compete on cybersecurity, it does return and become especially intense after learning of a cyberattack.⁹⁶

Furthermore, since the industry is extensively regulated, enterprises are hesitant to share information with the government regarding threats and vulnerabilities out of concern that it will result in audits or expose them to further liability. They are also anxious about how the information they contribute will actually be used in the context of an investigation, regulatory action or significant lawsuit.⁹⁷

The need for a more adaptive regulatory model (i.e. a strategy designed to facilitate routine learning, self-correction and adaptability to changing conditions over time) is indicated by the cyberspace's constant change. Yet, most regulatory approaches design solutions that are only re-examined when failure results in large enough costs to warrant high-level attention. It might be challenging to regulate a landscape of adaptative change over time because regulation frequently results in stagnant checklists.⁹⁸

Furthermore, even though CEOs are becoming more aware of the dangers of cyberattacks, many still see cybersecurity as primarily an IT issue, and only a small number of boards of directors believe that strategic investments in cybersecurity may produce business value and a competitive advantage.⁹⁹ For those who hold that belief, security spending encourages businesses to increase their investment because it gives them confidence they are safe from their rivals.¹⁰⁰ As a result, enterprises that invest in this way seem to be more competitive in the long run, because even if competitors eventually catch them up, the time lag is far greater than it would have been if they had not taken the measures to protect themselves.¹⁰¹

⁹⁶ Atkins and Lawson (n 7).

⁹⁷ Ibid.

⁹⁸ Ibid.

⁹⁹ Dejan Kosutic and Federico Pigni, 'Cybersecurity: Investing for Competitive Outcomes' (2020) 43 Journal of Business Strategy.

¹⁰⁰ Armando R. Gomes and others, 'Analyst Coverage Networks and Corporate Financial Policies' (2017) available at SSRN 2708935.

¹⁰¹ Benn Lawson and Danny Samson, 'Developing Innovation Capability in Organisations: A Dynamic Capabilities Approach' (2001) 5 International Journal of Innovation Management; Donald Mitchell and Carol Coles, 'The Ultimate Competitive Advantage of Continuing Business Model Innovation' (2003) 24 Journal of Business Strategy.



Yeh and Chang recently claimed that the scope of the countermeasures many businesses adopt does not correspond to the seriousness of the perceived threats. To remedy this, they proposed that organisations should assess the possible loss of value brought on by a security breach using estimations, allowing them to invest in information security measures that are proportionate to the anticipated loss.¹⁰²

If the goal is to try to avert every conceivable incident, then budgets will never be sufficient. While it may be necessary to invest more money, it is probably more important for businesses to invest with a focus on risk mitigation. Efforts should be made to identify the organisation's key assets and areas at risk and to model plausible attack scenarios. This supports appropriate decision-making on reasonable investments in the business's various divisions.¹⁰³

Some believe that increased development of cybersecurity calls for expanded and deeper (more operation-level) public-private cooperation, enabling businesses to make use of a wider and more useful array of government resources and instruments. In the long term, it is proposed that successful cybersecurity will depend more on consistent improvement than it will on following a set of rules.¹⁰⁴

3. Evaluating disclosure as a strategy to protect investors

The impacts of disclosure and its general desirability are rather equivocal in the academic literature. It is commonly known that disclosures can advance some of businesses' significant objectives, including lowering the cost of capital for businesses, raising market liquidity and efficiency and levelling the playing field in the financial markets. Destroying risk-sharing opportunities, encouraging the destabilising of beauty-contest incentives and crowding out private information generation are just a few of the further unintended effects of disclosure that have been extensively discussed in the literature. Recently, researchers have been delving deeper into the subject, to comprehend the benefits and drawbacks and provide answers to investors' important questions¹⁰⁵, including: what are the benefits of disclosure? How can the disclosures be effective? What is the best way to disclose information?

¹⁰² Goel and Shawky (n 74).

¹⁰³ Emily Mossburg, John Gelinne and Hector Calzada, 'Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts' (2016).

¹⁰⁴ Atkins and Lawson (n 7).

¹⁰⁵ Itay Goldstein and Liyan Yang, 'Information Disclosure in Financial Markets' (2017) 9 Annual Review of Financial Economics.



This chapter will outline the background to the topic of disclosures, for a comprehensive understanding of the beginnings of disclosures and how they concern investors. The focus will be on the ways disclosures can be made and the associated processes, which affect the various impacts disclosures may have. Chapter 2 noted the responsibility investors have to mitigate losses, and this chapter will present insights from the person who is responsible if a disclosure goes wrong. Finally, the chapter will present the advantages of disclosures that boost investors' confidence, painting a comprehensive picture of the approaches to making such a disclosure and the negative effects that could result. Overall, this chapter supports the reader to build a nuanced, realistic picture of disclosures and the scenarios in which they are made.

3.1. Background to disclosures

The primary focus of regulatory efforts to support the stability and quality of the financial markets is on information disclosure. Since the adoption of the Securities Act of 1933 and the Securities Exchange Act of 1934, the United States federal government has aggressively regulated US equities markets, according to Greenstone, Oyer and Vissing-Jorgensen.¹⁰⁶ Its requirement placed on the disclosure of financial information is the focal point of these efforts. The SOX Act of 2002 and the Dodd-Frank Act of 2010 both strongly emphasised various areas of increased disclosure, standing as recent, visible markers of the efforts made to improve related regulation in recent years. The earlier of the two, the SOX Act, was created to 'protect investors by increasing the accuracy and dependability of corporate disclosures made pursuant to the securities laws, and for other objectives'.¹⁰⁷

Following its enactment, a different branch of the federal government sought to advance security in the digital sphere in October 2011. The Division of Corporation Finance of the SEC released a staff document titled "Disclosure Guidance Topic No. 2—Cybersecurity", which set forth the SEC staff's views on public companies' obligations to disclose cybersecurity risks and cyberattacks, in response to pressure from the Senate Commerce Committee and a wave of widely publicised attacks on public companies. Companies registered with the SEC were already expected to disclose important information for the benefit of investors in their registration statements and periodic reports according to the Securities Acts of 1933 and 1934. Yet, for the first time, the Disclosure

 ¹⁰⁶ M. Greenstone, P. Oyer and A. Vissing-Jorgensen, 'Mandated Disclosure, Stock Returns, and the 1964 Securities Acts Amendments' (2006) 121 The Quarterly Journal of Economics.
 ¹⁰⁷ Goldstein and Yang (n 105).



Guidance established that the SEC regarded cybersecurity-related information as 'material' necessitating disclosure.¹⁰⁸

Policymakers expressed a strong desire to evaluate the guideline soon after it was released, over two years ago. Sen. John D. (Jay) Rockefeller IV asked SEC Chairwoman Mary Jo White in a letter written in April 2013 to "elevate Disclosure Guidance and issue it at the Commission level", to "send a strong signal to the market that companies need to take their cybersecurity efforts seriously". He also expressed his gratitude for the effectiveness of the Disclosure Guidance. As discussed infra, Senator Rockefeller played a significant role in advocating for cyber disclosure guidance. Chairwoman White responded by stating that she would assess "existing disclosure processes and overall compliance with the guidance and recommendations... for additional action in this area".¹⁰⁹

Despite objecting in writing to the SEC's interpretation of the relevant law or claiming that the information was not 'material' and not required to be disclosed, the registrants were forced to begin complying with the SEC's demands and now disclose more information about cyberattacks than they wish. Failure to comply with the Disclosure Guidance involves considerable risks because the SEC may take enforcement action against a corporation for failing to disclose material information, and shareholders may pursue a lawsuit for similar reasons.¹¹⁰

The SEC's guidelines have played a major role in the rise of cybersecurity disclosures on the global stock market landscape. A second SEC guideline on disclosing cybersecurity risks was released in 2018. After three years, in June and August 2021, the US Securities Commission issued firms the first penalties for lax disclosure controls and processes connected to cybersecurity risks.¹¹¹

Disclosure in financial markets has three core objectives: (i) it protects investors, and thud, by enhancing their confidence in the market, preserves the good functioning (if not the very existence) of the (securities) market, thereby supporting its growth; (ii) it addresses the problems of agency concerning large corporations, providing transparency around how they are organised, financed and operating; (iii) it ensures that prices fully reflect all value-relevant information, to help

¹⁰⁸ Ferraro (n 25).

¹⁰⁹ Ferraro (n 25).

¹¹⁰ Ibid.

¹¹¹ Ramírez and others (n 35).



financial markets in their fundamental function of efficiently allocating scarce financial resources across the economy.¹¹²

The fairness rationale has been almost universally discarded. Today, nobody seriously argues that protecting investors via disclosure is a proper policy simply because doing so is... just. Many, instead, and especially policymakers, contend that protecting investors is instrumental to the good functioning—if not the very existence—of the markets, warranting an efficiency justification. Providing investors with adequate protection increases their confidence in the markets. Alternatively, without a strong and widespread belief in market integrity, the investing public would withdraw its savings, with disastrous consequences for the entire economic system.¹¹³

Disclosure protects investors in three main ways: first, by providing them with all information reasonably needed to decide how to invest their savings, considering a security's risk and expected returns, the issuing entity, the attached rights and so forth. Thus, disclosure helps investors find the kind of investment that best matches their preferences, thereby minimising the risk of making poor investment decisions due to insufficient information regarding the securities purchased or sold.¹¹⁴

Second, disclosure may protect investors by enabling them not to be 'exploited' by traders with superior information, such as insiders and professional investors. According to this view, without disclosure, amateur investors would systematically lose out when trading against such informed counterparts, soon leading them to withdraw their money from the market. Disclosure is said to establish a "level playing field" between amateur and professional investors or corporate insiders, to give the former "equal access" to the same range of information on which the latter base their decisions.¹¹⁵

Third, disclosure protects investors by discouraging fraud, self-dealing and various other kinds of opportunistic behaviour on the part of managers and controllers. From this standpoint, the goal of investor protection aligns with improved corporate governance, which is addressed in the next section.¹¹⁶

¹¹⁵ Enriques and Gilotta (n 112). ¹¹⁶ Ibid.

¹¹² Luca Enriques and Sergio Gilotta, 'Disclosure and Financial Market Regulation' (2014) SSRN Electronic Journal.

¹¹³ Ibid.

¹¹⁴ Ibid.



Although, technically speaking, the SEC Disclosure Guidance relating to cybersecurity is not a binding mandate, citing the optional nature of disclosures will give a weak defence in the event of an investor lawsuit. In contrast to the SOX Act of 2002, which strongly emphasises computer-based information systems, and is, therefore, focused on cybersecurity inputs, the SEC Disclosure Guidance is concerned with cybersecurity outputs, namely cybersecurity risks and incidents.¹¹⁷

In their 2010 study, Gordon et al. evaluated voluntary disclosures of information on security and corresponding market valuations between 2000 and 2004 and discovered a strong correlation between the two. Yet, their sample period predated both the SEC's mandates for obligatory risk reporting, which took effect in 2005, and its supplemental guidelines on cybersecurity disclosures, effective from 2011.¹¹⁸ Gordon et al. proposed that in the early period under study, organisations that voluntarily disclosed information about cybersecurity risks demonstrated a commitment to mitigating those risks and thus enjoyed higher market valuations.¹¹⁹

Cybersecurity risk disclosures' release and duration, between the attacks and disclosing, are positively correlated with the chance of the firm subsequently reporting cyber-security incidents, according to Li et al., but this correlation was only found before the SEC's 2011 cybersecurity Disclosure Guidance came into force. The researchers contended that because these disclosures forecast that cybersecurity incidents were at risk of occurring, disclosures were instructive during the pre-guidance period.¹²⁰

However, in the post-guidance period, cyber disclosures are no longer indicative of cybersecurity incidents to follow, possibly as a result of a rise in the disclosures of inconsequential cybersecurity concerns. This trend casts doubt on how informative cyber disclosures are under the post-guidance system.¹²¹ Alternatively, the informativeness observed by Gordon et al. may have persisted after the guidelines were introduced, albeit with a wider impact on market valuations, given the more general nature of cyber disclosures in recent times.¹²²

¹¹⁷ Gordon and others (n 8).

¹¹⁸ Berkman and others (n 45).

¹¹⁹ Gordon and others (n 8).

¹²⁰ Gordon, Loeb and Sohail (n 48); Berkman and others (n 60).

¹²¹ Li, No and Wang (n 21).

¹²² Gordon, Loeb and Sohail (n 48); Berkman and others (n 60).



Many cyber-related disclosures made in the post-guidance period have taken the form of 'boilerplate' statements that were ambiguous or unspecific,¹²³ and as such, were uninformative to the market and of little importance or value. Finding these reports has become more challenging, too, as a result of the SEC's unclear guidance on what constitutes a 'disclosure' of a cyber event, concern or risk.¹²⁴

Nevertheless, senators, professionals and executives hailed the new SEC disclosure standards for cybersecurity as making a substantial change with far-reaching repercussions that had been pushed for by regulators. Senator John Rockefeller, for instance, described how "intellectual property worth billions of dollars has been stolen by cyber criminals, and investors have been kept completely in the dark. This guidance changes everything, it will allow the market to evaluate companies in part based on their ability to keep their networks secure. We want an informed market and informed consumers, and this is how we do it". Reading into this, the significant economic costs of cyberattacks appeared to be the primary driver of his interest.¹²⁵

In the European capital market, the cybersecurity and privacy laws, which include the GDPR and the directive on network and information systems security (NIS), may be interpreted to require the disclosure of cyber events. The obligation to disclose data incidents from a cybersecurity law perspective could incentivise the board to include information on this topic in the firm's annual financial reports, according to Eijkelenboom and Nieuwesteeg, even though doing so is not specifically mandated.¹²⁶ Yet, the archiving methods for disclosures may require further regulation still to come if we are to implement consistent systems in practice.

3.2. Ways of making disclosures

According to the 2011 Cybersecurity Guidance, a registrant must provide disclosures that are specific to their individual situation: "Registrants should avoid disclosing risks that may apply to any issuer or any offering and should avoid presenting hazards that could apply to any issuer". That is to say, registrants should offer information customised to their specific circumstances and avoid a generic 'boilerplate' disclosure. In addition to reiterating this point, the guidance sets forward the level of disclosure that is appropriate.

¹²³ Hilary, Segal and Zhang (n 87).

¹²⁴ Berkman and others (n 60).

¹²⁵ Hilary, Segal and Zhang (n 87).

¹²⁶ Ramírez and others (n 35).



The federal securities laws do not compel a registrant to make disclosures that might jeopardise their cybersecurity. Instead, registrants should disclose enough so that investors can understand the types of risks that specific involved, without the disclosure having that potential negative effect.¹²⁷

So, to prevent cybersecurity compromise through disclosure, concealment through generalisation was somewhat expected and advised against. However, since a registrant is allowed to consider the "adequacy of preventative activities" when determining the magnitude of a cybersecurity risk, it can be argued that only those who believe their own measures to be insufficient are ultimately required to submit risk information. Then, even a broad disclosure may signal to the hacker underground community that the company is weak. Additionally, it can suggest to the financial community, authorities and possible claimants in lawsuits that the company may not be adequately protecting its assets.¹²⁸

It seems, as a result, that firms seeking to implement the advice face a difficult decision. Businesses that adhere to the recommendations will be acknowledging a risk that is specific to their industry and recognising that it is "among the most important elements that make an investment in the firm speculative or dangerous". The disclosure identifies a vulnerability that the business cannot sufficiently address through preventative measures. The recommendations state that appropriate disclosures should cover "discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences", and "the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks". From a security standpoint, it does not seem appropriate to provide comprehensive information on either of these objects. Of course, the guidance specifically disclaims that securities rules are not intended to compromise a firm's cybersecurity, but surely this scenario will only be prevented if the firm is taking proper precautions. The underlying issue is that details of cybersecurity risks are what both investors and hackers seek to learn.¹²⁹

On the contrary, as long as it does not indicate a security issue, merely outlining generalised hazards that may apply to others in the same business seems relatively harmless. However, such a

¹²⁷ Morse, Raval and Wingender (n 50).

¹²⁸ Morse, Raval and Wingender (n 50).

¹²⁹ Morse, Raval and Wingender (n 50).



disclosure may also be largely ineffective, which is probably why the advice discourages firms from making one. Although a company might use such a disclosure to credibly convey to investors that the management takes cyber-risks seriously, that would involve going against the guidance to avoid releasing 'boilerplate' generic disclosures. For many businesses, remaining silent may be the best course of action, especially if they are taking the necessary procedures to address recognised threats and classing those threats as 'not material'.¹³⁰

Congress passed laws that provided a basic framework for disclosure, leaving it up to the SEC to establish more specific regulations. Form 10-K has become the required format for yearly reporting. Furthermore, at the conclusion of each of the first three fiscal quarters of each year, quarterly reports are required on Form 10-Q. In addition, on Form 8-K, which is only filed when specific material events occur, the current reporting may be required or permitted to be included. Forms 10-K, 10-Q and 8-K serve as the cornerstone for periodic reporting by domestic registrants, providing a means to inform investors, even though many other forms may be utilised for registrants with other particular characteristics.¹³¹ Disclosures may be required on several sections of the 10-K filings, including the Risk Factors, Management discussion and analysis (MD&A), Description of Business, Legal Proceedings and Financial Statement Disclosures (e.g. material prevention costs, or losses sustained) sections.¹³²

Periodic reporting requirements place a heavy load on registrants. According to government estimates, each firm must spend an average of 1,998.78 hours annually complying with Form 10-K. Form 8-K, only filed when specific material events occur, takes an average of 5.71 hours per response, and Form 10-Q, which must be filed three times annually, requires 187.43 hours per response on average.¹³³

To add to those, the SEC created Regulation S-K, an integrated framework for disclosures detailing both registration and ongoing reporting responsibilities, as a result of worries about efficiency, effectiveness and compliance difficulties. The SEC staff finished compiling the Regulation S-K disclosure requirements in December 2013 and it has since been in effect.¹³⁴ Yet, although it

¹³⁰ Morse, Raval and Wingender (n 61).

¹³¹ Ibid.

¹³² Hilary, Segal and Zhang (n 87).

¹³³ Morse, Raval and Wingender (n 61).

¹³⁴ Morse, Raval and Wingender (n 61).



mandates that corporations must report all significant risks, the guidance does not specifically address the disclosure of cyber-risks, threats or attacks.¹³⁵

Regardless of the forms and regulations now in place, managers remain strategic in their disclosure behaviour.¹³⁶ When it comes to specific cyber hazards, firms may become more vulnerable to assaults if they disclose too much or too precise information about them.¹³⁷ However, higher disclosure may also lower the likelihood that a breach will result in a lawsuit.¹³⁸ To walk the line between the two, the management may simply mention weak points in general terms when evaluating the company's material concerns.¹³⁹

By using 'boilerplate' language that does not truly provide specific details, managers may, for instance, avoid disclosing confidential information about risks¹⁴⁰, or they may concentrate the conversation on significant concerns that the company is currently addressing. Accordingly, Gordon et al. speculated that an increase in cybersecurity spending will go hand in hand with the increased reporting of cybersecurity-related activities as a result of the SEC's 2011 guidance.¹⁴¹ Such a trend reflects businesses concentrating the discussion on favourable aspects of cybersecurity. In this way, cyber-related disclosures become linked to the firms' cybersecurity awareness, given the significant dangers connected with disclosing vulnerabilities.¹⁴²

Businesses must include, under Item 1A of Form 10-K, "the most significant characteristics that make the offering speculative or risky", according to the SEC. This is required to "present investors with a clear and succinct explanation of the material risks to an investment in the issuer's securities". Yet, since companies are only obligated to offer qualitative descriptions and not to quantify the likelihood or impact of the disclosed risks, they have a great deal of discretion over what information to reveal and how to present it. Since managers frequently report risks using

¹³⁵ Berkman and others (n 60).

 ¹³⁶ Ronald A. Dye, 'Disclosure of Nonproprietary Information' (1985) 23 Journal of Accounting Research;
 Robert S. DeWoskin, 'Information Resources on Quality Available on the Internet' (2003) 10 Quality Assurance.
 ¹³⁷ Jonathan L. Rogers and Andrew Van Buskirk, 'Shareholder Litigation and Changes in Disclosure Behavior' (2009) 47 Journal of Accounting and Economics.

¹³⁸ Gordon, Loeb and Sohail (n 48).

¹³⁹ Berkman and others (n 60).

¹⁴⁰ Ronald A. Dye, 'Disclosure "Bunching" (2010) 48 Journal of Accounting Research.

¹⁴¹ Gordon and others (n 8).

¹⁴² Berkman and others (n 60).


imprecise words and list all the uncertainties they encounter, to disguise those of importance, practitioners criticise managers for giving investors little information.¹⁴³

In a similar vein, Robbins and Rothenberg proposed that risk factor disclosures are the least expensive type of insurance, especially when deliberately completed incorrectly, since when the contents of completed forms are later pulled up in court, "firms that cannot point to such a risk factor when faced with a lawsuit" will come under legal protection. This implies that companies have an incentive to make unhelpful disclosures of risk factors. The SEC sent out comment letters as soon as they became aware of the matter, asking businesses for more risk information and urging them to "avoid risk factor disclosure that may apply to any issuer or any offering".¹⁴⁴

Updates on risk factors have been the subject of several recent research studies. According to Filzen, companies that included risk factor updates in their quarterly reports had lower anomalous returns near the filing dates, fewer future unexpected earnings and a higher possibility of experiencing a future negative earnings shock.¹⁴⁵ Similarly, a second study by Filzen et al. showed that quarterly risk factor updates were negatively connected with future returns and that the association was larger for firms employing more direct language relating to firm fundamentals.¹⁴⁶

Furthermore, ex-post disclosures of data security breaches highly correlate with downward stock price movements, according to prior studies, and these correlations can last for lengthy periods. A breach disclosure most typically signifies fresh information reaching the market that could negatively impact the firm's financial outlook. Loss of investor trust in the management's capacity to protect the company's assets, as well as exposure to transaction costs associated with resolving claims, may detrimentally impact stock values.¹⁴⁷

Gaulin highlighted the significance of reporting individual risk factors, demonstrating that managers add new risk factors and delete stale risk factors in a timely fashion, and such activities predict future economic changes even after controlling for the ex-ante risk and company performance.¹⁴⁸ Furthermore, corporations respond to SEC comment letters by increasing the

¹⁴³ Li, No and Wang (n 21).

¹⁴⁴ SEC Disclosure Regulation 2010; Li, No and Wang (n 21).

¹⁴⁵ Joshua J. Filzen, 'The Information Content of Risk Factor Disclosures in Quarterly Reports' (2015) 29 Accounting Horizons.

 $^{^{\}rm 146}$ Li, No and Wang (n 21).

¹⁴⁷ Morse, Raval and Wingender (n 61).

¹⁴⁸ Maclean Peter Gaulin, Risk Fact or Fiction: The Information Content of Risk Factor Disclosures (2017).



clarity of their reportage, whereas they respond to securities lawsuits by increasing the number of risks they identify without increasing the definitiveness of their disclosures.¹⁴⁹

The SEC has utilised comment letters to compel disclosures of cybersecurity risks, even though the guidance specifically states that it is not a judgement. For instance, the SEC wrote in a comment letter addressing Freeport-McMoRan Copper & Gold Inc.'s 2011 annual report: "We note that none of your risk factors, or other sections of your Form 10-K, specifically address any risks you may face from cyberattacks, such as attempts by third parties to gain access to your systems to compromise sensitive business information, to interrupt your systems or otherwise try to cause harm to your business and operations. In future filings, beginning with your next Form 10-Q, please provide risk factor disclosure describing the cybersecurity risks that you face or tell us why you believe such disclosure is unnecessary". One could contend that the disclosure recommendation is evolving into a disclosure requirement because the SEC's comment letters are frequently seen as de facto judgements.¹⁵⁰

Media stories on information security breaches, or what we refer to as "breach announcements", are a key source of information for investors. Breach notifications are often published on blogs, large media sites, etc. Investors' views on the impact of the breach may differ depending on the vocabulary used and other aspects of the individual media reporting. For instance, some publications might employ more precise phrases, whilst other articles may use ambiguous language instead, prompting varied responses from investors.

Additionally, different information security events may have different repercussions for the impacted company. Information security incidents are frequently categorised as those that compromise information availability, integrity or confidentiality. Depending on the type of information affected and the legal jurisdiction of the parties involved, availability-type incidents or attacks may most likely result in temporary income losses for a company, whereas confidentiality-type incidents often lead to legal action.¹⁵¹

¹⁴⁹ Li, No and Wang (n 21).

¹⁵⁰ Gerry H. Grant and Grant C. Terry, 'SEC Cybersecurity Disclosure Guidance is Quickly Becoming a Requirement' (2014) 84 The CPA Journal.

¹⁵¹ Tawei Wang, Jackie Rees Ulmer and Karthik Kannan, 'The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities' (2013) 23 Journal of Organizational Computing and Electronic Commerce.



Early studies on the motivations for disclosure found that full disclosure occurs when there is no cost to disclosing information because investors believe that firms that never make disclosures have the worst prospects.¹⁵² However, businesses only share information when the advantages outweigh the costs and it is inexpensive to do so. Alternatively, transparency may be utilised to lower ex-post reputational and legal costs resulting from negative news or a company's underwhelming financial results.¹⁵³ Certain such disclosures are required by SOX, while others are left to the discretion of the individual firm.¹⁵⁴

The language style (tone) was the main topic of research by Davis et al., who demonstrated how the stock market can respond to various linguistic styles. According to Balakrishnan et al., news pieces can be classified as press- or firm-initiated, with firm-initiated media prompting significantly worse market reactions than press-initiated media.¹⁵⁵ According to Tetlock et al., when estimating a firm's fundamentals, the textual material in news items provides qualitative information. Loughran and McDonald expanded on Tetlock et al.'s findings and demonstrated how an alternative negative word list might accurately represent the tone of financial material.¹⁵⁶ According to further research by Kothari et al. into news reports, analyst reports and annual reports, the volatility of the stock price is lower when the information is reported more favourably.¹⁵⁷

In response to the SEC's 2011 Cybersecurity Guidance, businesses appear to have reacted carefully. Although cybersecurity threats are ubiquitous across a wide range of industries, only a tiny proportion of the organisations potentially impacted by these risks appear to have made affirmative risk factor disclosures in response to the guidelines. Although not all businesses opt to include the phrase "cybersecurity" in their disclosures, its use is growing. Looking ahead, as this

¹⁵² Sanford J. Grossman, 'The Informational Role of Warranties and Private Disclosure about Product Quality' (1981) 24 the Journal of Law and Economics.

 ¹⁵³ Douglas J. Skinner, 'Why Firms Voluntarily Disclose Bad News' (1994) 32 Journal of Accounting Research.
 ¹⁵⁴ Wang, Ulmer and Kannan (n 151).

 ¹⁵⁵ Balakrishnan, Karthik, Anindya Ghose and Panos Ipeirotis, 'the Impact of Information Disclosure on Stock Market Returns: The Sarbanes-Oxley Act and the Role of Media as an Information Intermediary' (2008) WEIS.
 ¹⁵⁶ Tim Loughran and Bill McDonald, 'When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks' (2011) 66 the Journal of Finance.

¹⁵⁷ S. P. Kothari, Xu Li and James E. Short, 'The Effect of Disclosures by Management, Analysts, and Business Press on Cost of Capital, Return Volatility, and Analyst Forecasts: A Study using Content Analysis' (2009) 84 The Accounting Review.



phrase comes to be used more consistently by the management and their professional advisers, it is anticipated that this expansion in its inclusion in reportage will continue.¹⁵⁸

Yet, contrary to the idea that progress is being made, the empirical evidence suggests otherwise. Investors have been noted to penalise companies that include a new disclosure for cybersecurity and related risks, in response to the Cybersecurity Guidance, on the annual Form 10-K. This negative market response indicates that, at least from the firm's perspective, caution may remain the best course of action. Although some businesses may believe disclosures will be beneficial for showing that the management is aware of cybersecurity issues, the market reaction implies that investors instead receive a different, warning signal.¹⁵⁹

Businesses have the option to both comply with the Cybersecurity Guidance and opt to refrain from adding a new disclosure item because the guidance does not contain any new regulations demanding further disclosures be made. Securities regulators rarely interpret this quiet as an actionable statement, and those who chose to remain silent and make no further disclosures may infer that their cybersecurity activities are sufficient to manage the threats in their environment. Unfortunately, those who add cybersecurity risk factor disclosures may find that their message is misunderstood by the market, which typically results in a decline in the stock price as a result of more firm-specific risk being signalled. Silence is indeed golden, as it is said.¹⁶⁰

Yet, the SEC seems to think more needs to be done. Back in 2014, Commissioner Luis A. Aguilar stated that "there is no doubt that the SEC must play a role in this area. What is less clear is what that role should be". In a recent move, the agency censured RT Jones Capital Equities, a local investment firm, after a cyberattack revealed information concerning 100,000 brokerage clients. The SEC also unveiled a plan to assess how US-registered investment advisers and broker-dealers fare in terms of cybersecurity.¹⁶¹ These two moves represent efforts on the part of the SEC to improve the current approaches to making disclosures.

3.3. Impact of disclosing incorrectly (Rule 10b-5)

The company and the officers and directors in charge of its disclosures may be held liable for mistakes in and omissions from company disclosures. Failure to adequately oversee operations,

¹⁶¹ Morse, Raval and Wingender (n 61).

¹⁵⁸ Morse, Raval and Wingender (n 61).

¹⁵⁹ Ibid.

¹⁶⁰ Ibid.



and thus safeguard the firm's assets, exposes corporate directors to liability risk (in contrast to those directors who take responsibility for investors' losses, as covered in Chapter 2 Section 2).

Federal securities regulations do not mandate that registered companies disclose every significant fact that shareholders might be interested in learning about. Liability for failure to disclose can, nevertheless, be determined under section 10(b) of the Exchange Act, which makes it unlawful to "use or employ, in connection with the purchase or sale of any security... any manipulative or deceptive device or contrivance in contravention of SEC rules and regulations". Rule 10b-5, which implements this provision, then states: "It shall be unlawful for any person... to make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading... in connection with the purchase or sale of any security".¹⁶²

To prevent claims from misleading investors, the legislation specifically targets false statements of a material fact, as well as information that should not be omitted. To break Rule 10b-5, such unlawful assertions or omissions must be made. Courts have recognised an implied private right of action to enforce rule 10b-5, which has become the primary basis for damages paid in settlements and judgements as a consequence of private actions involving federal securities laws. Corporate directors are thus exposed to liability risk if they do not properly oversee operations and protect assets.¹⁶³

Investor damages that may not otherwise be actionable under federal securities laws may instead be remedied otherwise under state law. A shareholder derivative claim, rather than a securities class action, may be utilised to seek compensation for damages brought on by a board of directors' conduct or inaction when this results in a violation of fiduciary duty. Yet, the standard for responsibility in this sector is high, making it challenging for shareholders to hold directors accountable for losses, as was shown previously in Chapter 2.¹⁶⁴

3.4. Benefits of disclosure

Various estimates of market responses to publicly disclosed attacks can be found. When businesses immediately announced a cyberattack, their stock prices typically fell 0.33 per cent in the first

¹⁶² Ibid.
¹⁶³ Morse, Raval and Wingender (n 61).
¹⁶⁴ Ibid.



three days and 0.72 per cent in the following month. In contrast, when companies concealed an assault and third parties later learned about it, market values fell by a substantially greater amount—1.47 per cent in the three days following the attack's discovery and 3.56 per cent in the month that followed.¹⁶⁵

Companies often suppress information about more dangerous attacks, while they disclose information about less dangerous ones. Withholding firms have been noted to have poorer analyst coverage, weaker corporate governance and lower litigation risk than disclosing firms. They have a low likelihood of discovery since investors pay closer attention to companies with greater analyst coverage. Yet, such companies receiving investors' attention may have stronger corporate governance, meaning they are less likely to keep bad news from investors, so there is no withheld information to uncover. For these firms, the high legal risk of withholding information, and the anticipated loss associated with that, make disclosures an attractive alternative.¹⁶⁶

Home Depot announced in a statement that their credit card systems had been compromised on 8 September 2014. In a several months-long security incident, the corporation went on to lose 56 million customers' credit card details. On 6 November, the business disclosed that the compromise was more serious than it had initially believed. Ultimately, 53 million customers' email addresses were also stolen, according to Home Depot. A slight, temporary decline in the stock price was caused by the original statement, but nothing more.¹⁶⁷

In a statement made available to the public on 4 February 2015, Anthem acknowledged that nefarious hackers may have accessed its servers and seized control of 37.5 million records including personally identifiable information. On 24 February 2015, Anthem increased the total to 78.8 million people whose personal information had been exposed. As a result of the announcements, the firm's stock price briefly and slightly decreased.¹⁶⁸

Only one of the five most prominent cyber-breaches in recent years, which received widespread public attention, seems to have had a major effect on the associated company's stock price, and this effect was still only temporary, with the stock price later recovering. It seems, at least for

¹⁶⁷ Hilary, Segal and Zhang (n 87).

¹⁶⁵ Amir, Levi and Livne (n 39).

¹⁶⁶ Amir, Levi and Livne (n 39).

¹⁶⁸ Ibid.



corporate giants such as Anthem and Home Depot, that a cyber-breach must have a huge economic impact before it affects their stock price in any meaningful way.¹⁶⁹

Some scholars propose that despite the best efforts of various actors including the SEC, not all market cyber-dangers will be addressed. Appropriate disclosure remains crucial, but this is a sobering truth. The SEC itself has been the target of a number of successful malicious assaults and intrusion attempts that are ongoing, showing that these can be developed and directed at even the most reliable organisations. Market participants now regularly suffer high remediation costs, as well as regulatory, litigation and reputational issues, as a result of cyber events. Investors, customers and other significant stakeholders ultimately bear many of the expenses associated with these risks, including the costs of mitigation.¹⁷⁰

It is not all doom and gloom, however. An organisation can let the market know that it is actively working to avoid, detect and fix security breaches by voluntarily disclosing cybersecurity issues in its annual report. The net present value (NPV) of a company, and consequently, the value of its stock on the market, should both rise as a result of these signals. For instance, by reducing the uncertainty around conducting business online linked to cybersecurity concerns, these signals may boost consumers' willingness to engage in e-commerce. The predicted net cash flows of a company, as well as the company's NPV and market value, should rise as consumer confidence to conduct e-commerce with the company increases.¹⁷¹

Due to the reduction in liability brought on by the enhanced openness linked with disclosures, voluntary disclosures relating to cybersecurity may also help to reduce possible lawsuit expenses.¹⁷² Additionally, financially minded computer hackers who seek monetary rewards for their efforts may be reluctant to invest resources in attacking systems where there is a reduced likelihood of success and a higher cost. In either of these two scenarios, a company should retain more of its cash flows thanks to its voluntary disclosures relating to cybersecurity, which will raise the firm's NPV and market value.¹⁷³

¹⁶⁹ Ibid.

¹⁷⁰Jay Clayton, 'Statement on Cybersecurity' (VitalLaw, 20 September 2017) http://business.cch.com/srd/SEC_3.pdf> accessed.

¹⁷¹ Gordon, Loeb and Sohail (n 48).

¹⁷² Ron Kasznik and Baruch Lev, 'To Warn or Not To Warn: Management Disclosures in the Face of an Earnings Surprise' (1995) 113–134.

¹⁷³ Gordon, Loeb and Sohail (n 48).



Ultimately, by eliminating knowledge asymmetry between a firm's management and its investors, as well as among its investors, voluntary disclosures about a firm's cybersecurity may lower the firm's cost of capital.¹⁷⁴ Since the rate used to discount anticipated future cash flows will be lower (as it is dependent on the firm's cost of capital), a firm's NPV, and consequently, its market value will rise under this lower cost of capital scenario. If companies with chances to generate high returns cannot distinguish themselves from businesses with only opportunities to generate low returns, investors will support both at the same level, which is that associated with low returns. To indicate to the market their high return potential, organisations can create large profits by voluntarily disclosing information on their strong cybersecurity measures. Since at least one company has already benefited from voluntary disclosures about cybersecurity, other companies undoubtedly can as well.¹⁷⁵

In essence, managers must strategically decide whether or not voluntary disclosures about cybersecurity will benefit their company in terms of its market value. Managers may be aware of the need for them to make this decision given the obvious trend toward greater voluntary disclosures related to cybersecurity. However, nobody has yet conducted an empirical analysis to determine whether or not choices regarding voluntary disclosures have the desired effect of raising firms' value.¹⁷⁶

4. Conclusion

A robust cybersecurity regulatory framework and financial commitment ensure the safety and stability of the securities market. This dissertation determined how cybersecurity laws affected investor confidence in the banking industry. The relevant parts of SOX, GDPR and the SEC's financial regulation's cyber rules were included within the scope of the analysis. For cybersecurity plans to be successful, according to the findings presented in this dissertation, they must be built around adaptable regulations that consider the nature of the Internet while also increasing investment in the sector.

The importance of this research is indicated by the common acknowledgement that poor cybersecurity in financial markets around the world has a significant influence in the failure of

176 Ibid.

 ¹⁷⁴ Paul M. Healy and Krishna G. Palepu, 'Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure Literature' (2001) 31 Journal of Accounting and Economics.
 ¹⁷⁵ Gordon, Loeb and Sohail (n 48).



many securities prices and the decline in investor confidence. Despite the importance of cyber threats to financial markets, this sector received little attention. This dissertation demonstrated that a framework for cyber regulation and investments prioritising risk avoidance significantly contributes to national institutions' underappreciation of cyber challenges. Following the financial cyber incidents, a flurry of regulatory legislation aimed at preventing attacks was implemented. These measures primarily involved exposing previous attacks to safeguard investors and provide them with an opportunity to make a choice. Some now think that the regulation is insufficient because of several significant cyberattacks in recent years. Increasing investment in cybersecurity might be a viable approach to reducing these risks.

4.1. Content

This dissertation explored the role that cybersecurity protection plays in boosting investor confidence in the securities markets. Because the US offers a unique impact on the world and sets the bar for financial regulation for many countries, the US approaches are highlighted. As Chapter 2 showed, the risks in cyberspace are detrimental to financial markets, including much discussion on who should oversee protecting investors' interests. As a result, investors tend to be powerless to hold a particular person or organisation accountable if they lose their assets due to cyberattacks. For the security preparation projects to protect investors, which top executives must direct, every organisation member is expected to share joint ownership, responsibility, and accountability. However, the amount of regulatory attention given to the financial sector has diminished because cyberattacks have impacted financial rules. The continuing cyberattacks provided convincing evidence that legislation may be ineffective in protecting the securities markets compared to robust cyber investment efficacy.

To demonstrate the applicability of the disclosure strategy from actual regulation, in particular, the SEC, SOX, and Dodd-Frank Act, Chapter 3 reviewed available facts. The case studies presented suggested how disclosures minimise cyber risk in securities markets. The impact of disclosure on the environment of the financial industry was featured in Chapter 3, especially with markets that avoid disclosing because they do not want to reveal their status to the government, which could result in undesired remediation efforts. Also, the decision to disclose could be detrimental to share prices, which has important implications for the position of disclosure as a guideline to the markets. Finally, the chapter detailed the disclosure process and demonstrated that the defendant is charged



under regulation 10b-5, exposing company directors to liability risk if they fail to supervise activities and safeguard assets adequately.

4.2. Key findings

The following summarises the findings of the examination of cybersecurity regulation. Since the Cold War, cyberattacks evolved to be more sophisticated and intense, with financial infrastructure being a notable target. These incidents are increasingly common in this sector because most products rely on digital technology than on physical goods or paper money. Even though markets prioritise maximising investors' value, few studies consider the effects of investor data breaches on valuation. Evaluations of the market show that investments in cybersecurity have received only minimal attention. Also, many markets typically disregard the cost analyses of these situations, and the significant economic harm they can inflict is either disregarded or excluded from the standard definitions of cyberattacks. Another common adverse impact of regulation is the stagnation of checklists.

Investors are kept in the dark about the most harmful attacks, while managers only disclose information about less severe attacks. Furthermore, choices made by the corporate board to use personnel or technological solutions to address cybersecurity issues are likely to be safeguarded from liability claims lawsuits. Therefore, if the directors can demonstrate they behaved honestly, then accusations that they failed to monitor or exercise supervision over cybersecurity concerns are unlikely to succeed. Yet, markets are forced to work against information exchange on the risks and vulnerabilities even when they consider it beneficial because understanding these actions and security flaws is related to an organisation's competitive advantage. Also, markets are apprehensive about disclosing information about threats and vulnerabilities to the government for fear of being held further liable.

Multiple studies showed a connection between falling stock prices and unfavourable cybersecurity incidents. So, a data leak involving investors is likely to have one of two effects on the securities market. First, the market might react negatively to hearing about the breach, demonstrating that it is aware of the clear repercussions of breaches. Second, the news of a data breach may not cause the financial market to react significantly. Instead, the effect could be felt long-term or deeply, or the market is not disclosed. Moreover, most significant marketplaces have insurance to cover a portion of their cyber risk.



By assisting investors in selecting the investment type that most closely matches their preferences, disclosure lowers the risk of making "wrong" investment decisions, provides them with the ability to avoid being "exploited" by traders with better information and deters fraud. Even though these statements tend to be boilerplate comments that may be vague or unspecific, cyber disclosures made in the post-guidance era are uninformative to the market and less significant for valuation. Therefore, using boilerplate language does not offer more insight.

Studies showed that ex-post disclosures of data security breaches are highly correlated with declining stock price movements, and these relationships can last for an extended time. The decline in investor confidence in management's ability to safeguard the company's assets and exposure to the transaction costs related to resolving claims may negatively affect stock prices. Also, while the disclosure guidance explicitly indicates that it is not a judgement, the SEC has leveraged comment letters to compel cybersecurity risk disclosures.

Corporate directors are exposed to being held liable if they fail to follow section 10(b) of the Exchange Act's requirements for asset protection and disclosure operations oversight. Resulting from individual lawsuits involving securities regulations, this rule emerged as the primary basis for damages awarded in settlements and court rulings.

Unfortunately, those who include cybersecurity risk factor disclosures discover that their message is often misconstrued by the market, which results in decreased stock prices from other firm-specific risks being signalled. A common practice is keeping quiet when in doubt, so most markets may potentially comply with the Cybersecurity Guidance by choosing not to introduce a new disclosure item. The SEC appears to believe that more work needs to be done, so attempts to enhance the disclosure method are in progress.

However, with voluntary disclosure of cybersecurity situations, increasing the value of stocks on the market and lower litigation costs may be possible. Such a decision should be made by the managers. However, no empirical investigation has yet to be performed to ascertain if decisions regarding voluntary disclosures result in the desired effect of increasing market value.

4.3. Discussion

This investigation revealed a shortage of previous studies on the effects of investor data breaches. Valuation may be the first step markets need to take to comprehend the true impact of a cyberattack on investors' confidence. Because regulators seem to have recognised the impact of cyberattacks



on financial markets, these issues are now being addressed, which marks a significant turn in regulators' approach to developing current regulations. While considering why markets do not share their cyber data with researchers may be acceptable, structural adjustments to the sector create additional defences against a build-up of cyber risk.

The financial sector is complex and opaque due to the sector's dynamic nature, particularly in technological breakthroughs. This thesis illustrated how national efforts are progressing to organise cybersecurity within financial markets. However, global regulation or a clear strategy agreeable across all markets is required due to the way markets function and how they are interconnected globally to prevent an attack that would split the consequences among them.

In relation to investors and markets, managers may also be held to conflicting obligations, as they must consider their respective interests to avoid conflicts. For them, the market's stability comes first, and in some circumstances, investors' interests come second. Therefore, they should accept responsibility for their actions if they have affected investors' conditions while not discounting their good faith actions.

This dissertation demonstrated the significance of the cybersecurity concept in the financial market industry and the potential need for field expansion in the context of concept research. Attention was provided to how significant the impact cyberattacks may have that resemble an armed assault. The analysis demonstrated that when the concept expands, the need to safeguard investors and markets may receive more focus and serious consideration because investors would be regarded as citizens with markets perceived as public spaces.

The analysis of the dissertation also demonstrated that regulation must be replaced because it leads to stagnant checklists. On the other hand, markets can be encouraged to increase investment in cybersecurity for financial markets because it gives investors confidence that they are secure from competitors and attacks. Specifically, when the cybersecurity scale is advanced in the securities market, attacks may not be able to catch up. Therefore, continuous improvement instead of adhering to standards can be more important for cybersecurity success.

Given the widely acknowledged concerns about disclosure, a thorough re-examination of its effectiveness is necessary. There is no benefit to the common, unclear and shallow methods of disclosure, which do not provide usefulness to investors in making decisions, as is evident from the varied opinions presented in this research.



Future research must consider the practical ramifications of transparency to guarantee that such discoveries are advantageous. This dissertation supports this goal by describing the advantages and disadvantages of disclosure.

A successful plan must be devised to fulfil the disclosure's goals of maximising market and investor returns. Also, successful disclosures occurred before the 2011 financial markets rules. Therefore, determining how disclosure generates acceptable outcomes and benefits is crucial, accomplished through empirical market research and considering other perspectives to create a just and efficient balance in the market. Even if disclosure decreases stock values, the effect cannot be prevented because prices could eventually fall even if the disclosure is not made because information could eventually be discovered. The disclosure must be provided in a reasonable manner that is determined by the Securities Commission or other party based on solid foundations.

Finally, this dissertation demonstrated that the SEC left a systemic gap by failing to identify the party accountable for an incorrect disclosure. To improve our comprehension of the processes involved in cyberattacks on the securities markets, a more interdisciplinary study is required to identify the culprit, making it possible for disclosure to be viewed in a more nuanced and realistic light. Specifically, the investor could feel confident in regaining their right or holding those accountable for failing to uphold it accountable. Ultimately, in accordance with the SEC's policy of compulsion, it must modify or clarify the status of its regulations, even if they are not enforceable in the financial markets. In other words, the commission must be precise in its directions and avoid ambiguity, regardless if the phrasing indicates mandatory action.

5. Acknowledgements

Many thanks go to my supervisor, Dr Catherine Coleman, for her guidance on this project. I am also grateful to my family for their continuing support. Without them, this study would not be possible.

6. Table of Legislation

Sarbanes-Oxley Act 2002 Dodd-Frank Wall Street Reform and Consumer Protection Act New York 23 NYCRR 500 SEC Disclosure Regulation 2010 Securities and Exchange Act: Rule 10b-5 1934



7. Bibliography

- Amir E, S Levi and T Livne, (2018). 'Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets' 23 Review of Accounting Studies.
- Andoh-Baidoo F, K Amoako-Gyampah and K Osei-Bryson, (2010). 'How Internet Security Breaches Harm Market Value' 8 IEEE Security & Privacy Magazine.
- Arner D W, J Barberis and R P Buckey, (2016). 'FinTech, RegTech, and the reconceptualisation of financial regulation', Nw. J. Int'l L. & Bus. 37: 371.
- Atkins S and C Lawson, (2021). 'Cooperation Amidst Competition: Cybersecurity Partnership In The US Financial Services Sector' 7 Journal of Cybersecurity.
- Balakrishnan K, Ghose A and Ipeirotis P, (2008). 'the Impact of Information Disclosure on Stock Market Returns: The Sarbanes-Oxley Act and the Role of Media as an Information Intermediary' WEIS.
- Berkman H and others, (2018). 'Cybersecurity Risk Mitigation, Private Information Leakage and Earnings Announcements' (SSRN Electronic Journal, 1st December 2018) <<u>https://www.researchgate.net/profile/Jonathan-</u> Jona/publication/325752038 Cybersecurity Awareness and the Cost of Liquidity/links/ 5d726f0b92851cacdb23ff46/Cybersecurity-Awareness-and-the-Cost-of-Liquidity.pdf>

accessed.

- Berkman H and others, (2018). 'Cybersecurity Awareness and Market Valuations' 37 Journal of Accounting and Public Policy.
- Bosworth S and M Kabay (eds.) (2002). Computer security handbook.
- Callen-Naviglia J and James J. (2018). 'FinTech, RegTech and the Importance of Cybersecurity' Issues in Information Systems.
- Campbell K and others, (2003). 'The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market' 11 Journal of Computer Security.
- Cavusoglu H, B Mishra and S Raghunathan, (2004). 'the Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms And Internet Security Developers' 9 International Journal of Electronic Commerce.



- Cavusoglu H, H Cavusoglu and S Raghunathan, (2004). 'Economics Of IT Security Management: Four Improvements To Current Security Practices' 14 Communications of the Association for Information Systems.
- Chai S, M Kim and H Rao, (2011). 'Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior' 50 Decision Support Systems.
- Chatterjee D, (2019). 'Should Executives Go To Jail Over Cybersecurity Breaches?' 29 Journal of Organizational Computing and Electronic Commerce.
- Chatterjee P K, (2018). 'City Hosts a Highly-Heralded Cyber Security Event' Free Press Journal.
- Clayton J, (2017). 'Statement on cybersecurity' (VitalLaw, 20 September 2017) <<u>http://business.cch.com/srd/SEC_3.pdf</u>> accessed.
- Dahlgren S J, (2015). 'The importance of addressing cybersecurity risks in the financial sector' no.160.
- DeWoskin R, (2003). 'Information Resources on Quality Available on the Internet' 10 Quality Assurance.
- Dye R, (2010). 'Disclosure "Bunching" '48 Journal of Accounting Research.
- Dye R, (1985). 'Disclosure of Nonproprietary Information' 23 Journal of Accounting Research.
- Enriques L and S Gilotta, (2014). 'Disclosure and Financial Market Regulation' SSRN Electronic Journal.
- Ettredge M and V Richardson, (2003). 'Information Transfer among Internet Firms: The Case of Hacker Attacks' 17 Journal of Information Systems.
- Ferraro M, (2013). 'Groundbreaking' or Broken? An Analysis of SEC Cyber-Security Disclosure Guidance, Its Effectiveness, and Implications' SSRN Electronic Journal.
- Filzen J, (2015). 'The Information Content Of Risk Factor Disclosures in Quarterly Reports' 29 Accounting Horizons.
- Fischer E, (2014). 'Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation'
- Garg A, J Curtis, and H Halper, (2003). 'The Financial Impact Of IT Security Breaches: What Do Investors Think?' 12 Information Systems Security.



- Gatzlaff K and K McCullough, (2010). 'The Effect of Data Breaches On Shareholder Wealth' 13 Risk Management and Insurance Review.
- Gaulin M, (2017). *Risk Fact or Fiction: The Information Content of Risk Factor Disclosures* (Rice University 2017).
- Gervais M, (2012). 'Cyber Attacks and the Laws of War' Journal of Law & Cyber Warfare 1.
- Goel S and H Shawky, (2009). 'Estimating the Market Impact Of Security Breach Announcements on Firm Values' 46 Information & Management.
- Goldsmith J, (2007). 'Who Controls the Internet? Illusions of a Borderless World' 23 Strategic Direction.
- Goldstein I and L Yang, (2017). 'Information Disclosure in Financial Markets' 9 Annual Review of Financial Economics.
- Gomes A R and others, (2017). 'Analyst coverage networks and corporate financial policies' Available at SSRN 2708935.
- Gordon L and others, (2015). 'Increasing Cybersecurity Investments in Private Sector Firms' Journal of Cybersecurity.
- Gordon L, Loeb M and Sohail T, (2010). 'Market Value of Voluntary Disclosures Concerning Information Security' 34 MIS Quarterly.
- Gordon L, M Loeb and L Zhou, (2011). 'the Impact of Information Security Breaches: Has There Been A Downward Shift In Costs?' 19 Journal of Computer Security.
- Grant G and T Grant, (2014). 'SEC cybersecurity disclosure guidance is quickly becoming a requirement' The CPA Journal 84, no. 5.
- Greenstone M, P Oyer and A Vissing-Jorgensen, (2006). 'Mandated Disclosure, Stock Returns, and the 1964 Securities Acts Amendments' 121 the Quarterly Journal of Economics.
- Grossman S, (1981). 'The Informational Role of Warranties and Private Disclosure about Product Quality' 24 the Journal of Law and Economics.
- Healy P and K Palepu, (2001). 'Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure Literature' 31 Journal of Accounting and Economics.



- Higgs J and others, (2016). 'The Relationship Between Board-Level Technology Committees And Reported Security Breaches' 30 Journal of Information Systems.
- Hilary G, B Segal and M Zhang, (2016). 'Cyber-Risk Disclosure: Who Cares?' SSRN Electronic Journal.
- Hinz O and others, (2015). 'The Influence of Data Theft on the Share Prices and Systematic Risk of Consumer Electronics Companies' 52 Information & Management.
- Hovav A and J D'Arcy, (2005). 'Capital Market Reaction to Defective IT Products: The Case Of Computer Viruses' 24 Computers & Security.
- Hovav A and J D'Arcy, (2003). 'The Impact of Denial-Of-Service Attack Announcements on the Market Value Of Firms' 6 Risk Management and Insurance Review.
- Kabanda S, M Tanner and C Kent, (2018). 'Exploring SME Cybersecurity Practices in Developing Countries' 28 Journal of Organizational Computing and Electronic Commerce.
- Kashmiri S, C Nicol and L Hsu, (2016). 'Birds Of A Feather: Intra-Industry Spillover Of The Target Customer Data Breach And The Shielding Role Of IT, Marketing, And CSR' 45 Journal of the Academy of Marketing Science.
- Kasznik R and B Lev, (1995). 'To warn or not to warn: Management disclosures in the face of an earnings surprise' 113-134.
- Kaur G, H Z Lashkari and H A Lashkari, (2021). Understanding Cybersecurity Management In *Fintech*, (Cham: Springer, 2021).
- Kilovaty I, (2014). 'Rethinking the prohibition on the use of force in the light of economic cyber warfare: towards a broader scope of Article 2 (4) of the UN Charter', JL & Cyber Warfare 4: 210.
- Ko M and D Carlos, (2006). 'The impact of information security breaches on financial performance of the breached firms: an empirical investigation' Journal of Information Technology Management 17, no. 2 13-22.
- Kosutic D and F Pigni, (2020). 'Cybersecurity: Investing For Competitive Outcomes' 43 Journal of Business Strategy.



- Kothari S, X Li and J Short, (2009). 'The Effect Of Disclosures By Management, Analysts, And Business Press On Cost Of Capital, Return Volatility, And Analyst Forecasts: A Study Using Content Analysis' 84 The Accounting Review.
- Kubo Mačák, (2016). 'Is the international law of cyber security in crisis?' IEEE 8th international conference on cyber conflict (CyCon) 127.
- Lawson B and D Samson, (2001). 'Developing Innovation Capability in Organisations: A Dynamic Capabilities Approach' 05 International Journal of Innovation Management.
- Li H, W No and T Wang, (2018). 'SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors' 30 International Journal of Accounting Information Systems.
- Loughran T and B McDonald, (2011). 'When Is A Liability Not A Liability? Textual Analysis, Dictionaries, and 10-Ks' 66 the Journal of Finance.
- McNutt J, (2004). 'Analysis of the US-CERT DAC' Carnegie-Mellon University Pittsburgh Pa Software Engineering Inst.
- Mitchell D and C Coles, (2003). 'The Ultimate Competitive Advantage Of Continuing Business Model Innovation' 24 Journal of Business Strategy.
- Morse E A, V Raval and J R Wingender Jr., (2017). 'SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors' The Business Lawyer 73, no. 1 1-34.
- Morse E, V Raval and J Wingender, (2011). 'Market Price Effects Of Data Security Breaches' 20 Information Security Journal: A Global Perspective.
- Mossburg E, J Gelinne and H Calzada, (2016). 'Beneath the surface of a cyberattack: A deeper look at business impacts'.
- Pirounias S, D Mermigas and C Patsakis, (2014). 'The Relation Between Information Security Events And Firm Market Value, Empirical Evidence On Recent Disclosures: An Extension of the GLZ Study' 19 Journal of Information Security and Applications.
- Prince B, (2015). 'Shifting Priorities: How Enterprises are Safeguarding against Cybersecurity Threats' 196 Forbes 119–124.
- Ramírez M and others, (2022). 'The Disclosures Of Information On Cybersecurity In Listed Companies In Latin America—Proposal For A Cybersecurity Disclosure Index' 14 Sustainability.



- Robbins R and P Rothenberg, (2005). 'Securities disclosure' Insights: The Corporate & Securities Law Advisor 19, no. 5.
- Rogers J and A Van Buskirk, (2009). 'Shareholder Litigation and Changes in Disclosure Behavior' 47 Journal of Accounting and Economics.
- Sample C and others, (2017). 'Culture + Cyber: Exploring the Relationship' In Advances in Human Factors in Cybersecurity, 593:185–196. Cham: Springer International Publishing.
- Skinner D, (1994). 'Why Firms Voluntarily Disclose Bad News' 32 Journal of Accounting Research.
- Telang R and S Wattal, (2007). 'An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price' 33 IEEE Transactions on Software Engineering.
- Wang T, J Ulmer and K Kannan, (2013). 'The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities' 23 Journal of Organizational Computing and Electronic Commerce.
- Yadron D, (2014). 'Boards Race to Fortify Cybersecurity' the Wall Street Journal.
- Yayla A and Q Hu, (2011). 'The Impact Of Information Security Events On The Stock Value Of Firms: The Effect Of Contingency Factors' 26 Journal of Information Technology.

Copyright © 2023 Sumayah Saed S. Alsahafi, AJRSP. This is an Open-Access Article Distributed under the Terms of the Creative Commons Attribution License (CC BY NC) **Doi:** <u>https://doi.org/10.52132/Ajrsp.e.2023.54.1</u>



Risk and Return of NFT, Metaverse, Cryptocurrency, and NFT's Relation with IP

Author: Bodour Idris Radwan

MSc Finance, University of Business and Technology, Saudi Arabia Email: <u>bedourradwan92@gmail.com</u> | DOI: <u>https://orcid.org/0009-0004-0773-0724</u>

Co-author: Dr.Mohammed Binkhamis

Dar Al-Hekma University, Saudi Arabi

Email: m.binkhamis@ubt.edu.sa

Abstract:

This research discusses the Risk and Return of NFT, IP, Metaverse, and cryptocurrency. To investigate the factors affecting the risk and return of Cryptocurrency, Metaverse & NFT, and the connection between them. Being aware of the risk and return factors will help investors make the right decision and avoid these risk factors. The research studies the link between NFT and other digital assets. As well as, the relation between NFT and IP. Furthermore, explores the probability of NFT taking place in the Middle East. Qualitative Method was used to collect the primary data in the completion of this study. Data were collected using a survey strategy by interviewing investors, creators, and blockchain technology specialists through semi-structured interviews. The research time horizon across-sectional study. As well as secondary sources to help explain the concepts and support the primary data. After having analyzed the information, that has been gathered regarding the topic of discussion, it has come to the result that the NFT is digital proof of ownership, that is used in digital or real assets if legally approved. Besides, risk and return factors affecting NFT, Metaverse, and cryptocurrency are very close with small differences in cryptocurrencies as it is a wide market. Furthermore, there is a huge potential for taking place in the Middle East. Which creates new investment opportunities.

Keywords: NFTs, Metaverse, cryptocurrency, IP, risk



1. Introduction

1.1. About the digital assets

A digital asset is anything that is digitally recorded and uniquely identifiable and may be used by organizations to generate value. Its representations of values are not issued or guaranteed by a central bank or public authority and do not have the legal status of currency or money.

The blockchain has inhaled new life into the term. An entire class of advanced resources in the blockchain is being created, and it's possibly the main speculation opportunity since the Internet.

It is important to understand the new class of digital assets for the creation of smart investment strategies, improvement of new organizations, and broadening conventional portfolios. As such, assuming that you might want to contribute and develop your abundance of the blockchain, you want to see each sort of advanced it is today.

1.2. Type of blockchain digital assets

For one reason, digital assets provide a trillion-dollar investment opportunity. The ultra-fast digital economy necessitates entirely new approaches to wealth creation and corporate operations.

Whether it's crypto commodities, cryptocurrencies, security tokens, utilities, or real-world asset tokens, the digital asset blockchain enables the global economy to be overhauled and redesigned, increasing efficiency and opening the door to incredible new prospects.

The five basic forms of digital assets now available on the blockchain are listed in Figure 1.



(Warmann,2020)





1.3. Fungible and non-fungible assets

What are fungible and non-fungible assets? fungible assets are assets that can be exchanged for something else or to equal value they could be: currencies, commodities, and precious stones. On the other hand, non-fungible assets: is an asset that has unique proper that cannot be interchanged elsewhere. It could be a painting that is one of a kind Orkin uses. You can snap a picture of the work of art or purchase a print however there will just at any point be one unique painting.

1.4. NFTs

NFTs (Non-Fungible Tokens) are a type of digital authentication instrument. NFTs are known to be the most popular particulars the s in today's world. These objects have been authenticated. NFTs are analogous way, but they only live in the digital realm. Preliminarily, no technology was to allow for the power of digital means.

1.5. Metaverse

The Metaverse is a virtual open area created by combining virtual reality with digital reality. Activities that currently take place in isolated locations (such as purchasing digital land and building virtual homes, participating in a virtual social experience, and so on) will eventually move to the Metaverse. As well as Metaverse works with a variety of technologies.

1.6. Cryptocurrency

Cryptocurrency is a type of digital payment that does not require transaction verification by a bank. Cryptocurrency payments are digital entries in an online database that identify individual transactions, rather than physical money that may be carried about and exchanged. The cryptocurrency is kept in a digital wallet.

1.7. Aim

To investigate the factors affecting the risk and return of Cryptocurrency, Metaverse & NFT, and the connection between NFT, IP, Metaverse, and Cryptocurrency.

1.8. Purpose of study

The goal of the study is to investigate the new financial instrument and their relations. Moreover, studying the NFT relation with each of the following IPs, Metaverse, and Cryptocurrency. Furthermore, studying the risk and return of all of them helps investors make the decision and choose where or in which index will invest.



Also, research on the potential of NFT takes place in the Middle East.

1.9. Research questions

Is NFT a form of currency, a commodity, a stake in a technology breakthrough, or a completely different instrument?

What are the factors affecting the risk and return of NFT, Metaverse, and cryptocurrency to help investors make the decision?

Components what is the intersection and division of NFT, IP, Metaverse, and cryptocurrency?

How common are non-fungible tokens in the Middle East?

1.10. Objectives

- To introduce NFT, Metaverse & cryptocurrency
- To investigate risk and return affecting NFT, Metaverse & cryptocurrency
- To highlight the relationship between NFT and IP
- To discuss the relationship between NFT, cryptocurrency & Metaverse
- To discuss the investment opportunity on NFT
- To help the investors reach their goal which is to increase wealth
- To help the investors make the right investment decision depending on risk and return analysis.

2. Literature review

Subject introduction: Risk and return of cryptocurrency, Metaverse & NFT and its association with IP

Why choose the Risk and Return of Cryptocurrency, Metaverse & NFT, and its association with IP as a topic?

The topic was chosen because of the hype happening in this field and the different points of view about non-fungible tokens (NFT) nature. Highlighting the relation between NFT and IP, the similarities and differences. In addition to the relationship of non-fungible tokens to both the Metaverse and digital currencies. This chapter includes a Literature Review and secondary data related to researcher questions.



What is NFT is it a form of currency, a commodity, a stake in a technology breakthrough, or a completely different instrument?

NFTs are not cryptocurrencies. NFTs are not cryptocurrencies. Although the two assets are considered digital assets under the same umbrella, they have distinct qualities that distinguish them. (Omariba 2021)

A Blockchain-based technological breakthrough that revolutionizes digital ownership for art, collectibles, and gaming. NFT is a huge technology innovation that allows for new online behavior, paving the door for new business models and investment opportunities, since economic rewards may be collected in previously unimaginable ways. (Finucane, 2021)

Another possible regulatory difficulty, according to Washington, D.C.-based securities partner Josh Sterling, is whether the NFT is a commodity. "Except onions and box office receipts from movie theatres, almost anything is a commodity under the Commodity Exchange Act, says one expert. he argues. "As a result, it's quite possible that the Commodity Futures Trading Commission will decide that NFTs are commodities". (Acello, 2021).

What are the factors affecting the risk and return of NFT, Metaverse, and cryptocurrency to help investors make the decision?

NFT risk and return

Individuals and enterprises working in these areas should carefully assess the benefits of owning an NFT platform or portfolio, as well as new applications of and maybe revisions to current bodies of legislation, such as copyright and false advertising, that will handle NFT challenges. (Business Management)

Metaverse risk and return

Metaverse has caused quite a stir in the decentralized space. It's not just about playing NFT games to immerse oneself in a virtual environment; it's also about investing in cutting-edge technology. Investing in the Metaverse, on the other hand, is only worthwhile if you have the necessary knowledge and abilities to evaluate the industry and market. The Metaverse comes with its own set of dangers and benefits.

If you want to enjoy the advantages, you must take risks. However, calculated risk.

The Metaverse risks are Limited Market, risk of losing the investment, and Scams as explained in Figure 2.

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54

Publication Date: 05-10-2023 ISSN: 2706-6495



The Market for	Risk Of Losing Your	Risks With Metaverse
Metaverse Is Limited	Investment	Scams
• Only those who are interested in the niche will invest in the Metaverse. You must bear in mind that your market is tiny and constrained.	 The platforme could get away. Even if you have NFTs confirming your ownership, no government recognizes or authorizes them. 	• Check the authenticity of the land NFT, its owners and the platform it exists on.

Figure (2) The Metaverse risk

Based on our study and statistics from New ZOO, IDC, PWC, Statista, and Two Circles, the worldwide Metaverse revenue opportunity might surpass \$800 billion in 2024, up from over \$500 billion in 2020. The principal market for online game producers and gaming equipment might reach \$400 billion in 2024, with the rest coming from live entertainment and social media. (Bloomberg Intelligence, 2021)



Figure (3) Metaverse Market Growth

Also, according to financial services firm PwC, the global Metaverse market will grow from \$148.5 billion last year to \$476.4 billion by 2025 and \$1.542 trillion by 2030(PWC)

Cryptocurrency risk and return:

The risk of cryptocurrencies is high volatility, so it's too risky to invest in one currency.

Among others, a possible sanctuary for the transfer of unlawfully obtained cash Furthermore, the historically high returns generated by cryptocurrency investments throughout their short lifespans have piqued the curiosity of both speculators and casual onlookers.



The potential rewards are great when compared to more traditional assets like foreign currencies and the stock market, and the hazards are proportionately bigger (Cudd et al. 2018).

What are the intersection and division of NFT and each of the following IP, Metaverse, and Cryptocurrency?

Non-fungible tokens and intellectual properties

An NFT is not a type of intellectual property. It doesn't fit into any of the existing IP classifications. An NFT is closest to a form or proof. It merely verifies that the owner of the NFT owns the "real" or actual version or copy of something and it could have an infinite copy of it. (Chintalapoodi 2021)

Intellectual property is not a non-fungible token. An NFT is neither a kind of cash nor intellectual property in and of itself. The underlying digital picture, on the other hand, might be protected by copyright or a trademark. (Deepika and Dileep 2021)

Non-fungible tokens and Metaverse

In the Metaverse, NFTs may be used to represent ownership of in-game assets, virtual avatars, and real estate holdings (digital version). Similarly, the Metaverse-based NFT marketplace allows users' avatars to browse the marketplace, examine the digital items in greater detail, and select the product of their choosing. (Takyar 2022)

NFT and Metaverse Comparisons of Idea, fungibility, and benefit are clarified in Table 1.

Parameters of	NFT	Metaverse
Comparison		
Idea	The NFT idea is built on	The Metaverse idea is based on the sale
	blockchain technology, and users	and purchase of NFTs of various digital
	may purchase it using Bitcoin.	things.
Fungibility	NFTs are non-fungible tokens, as	The Metaverse currency will very
	the name implies since they are	definitely be a fungible token that can be
	one-of-a-kind in appearance.	traded and swapped for equivalent
		amounts of money.

Table 1. NFTs vs Metaverse



Benefit	NFT's most significant benefit is	Metaverse is expected to improve	
	that it gives content creators with	education by allowing students to	
	robust copyright protection.	participate in real-time active classrooms.	

Non-fungible tokens and cryptocurrency

An NFT is not a type of intellectual property. It doesn't fit into any of the existing IP classifications. An NFT is closest to a form or proof. It merely verifies that the owner of the NFT owns the "real" or actual version or copy of something and it could have an infinite copy of it. (Conti and Schmidt 2022)

In the Middle East, how frequent are non-fungible tokens?

Three Middle Eastern NFT markets raised roughly \$10 million last year. Now, Art Dubai, the region's largest art festival, is dedicating an entire area to digital art and NFTs. (Hamid, 2022)

"At the moment, there are not a lot of regional artists that are readily transitioning to NFTs or digital art, but I see that changing very soon," says Dubai-based contemporary artist, Kristel Bechara. "We will see an increasing number of local and worldwide artists using NFTs to sell their paintings shortly as a result of expanding popular interest and technology that is improving and becoming easier and more accessible." Bechara herself became the first Arab female artist to launch an NFT-tokenized art series in the UAE and the Middle East. It sold in less than 24 hours for approximately 1.10 ETH (\$2528).

NFT is also attracting the attention of other artists and galleries. This year, Kuwait's Gallery Bawa, a digital art gallery, had its inaugural NFT art exhibition. Abdullah Qandeel, a Saudi artist, claimed to have launched the world's first Artist-Approved Physical NFT on June 29 (AP-NFT). Elie Saab, a Lebanese international fashion house, has announced its entry into the Metaverse, where it has opened a virtual store, to provide a unique experience for its customers and to keep up with the world of digital development that we are witnessing at the moment, thus joining a group of luxury brands that have a tangible presence in the digital world of NFT. Dubai Police General Command launched its first set of non-fungible digital assets (NFT), consisting of 150 digital assets. MBC Group the largest media organization and the pioneer in the Middle East and North Africa launched the Genesis NFT collection, offering more than 200 properties of different levels of scarcity, in March 2022, in partnership with ENCORE Strategy a technology and marketing mentor company, based in Zurich, Switzerland, and AFTERMEDIA a media company for the development of trade and business (MBC).



3. Methodology

This chapter will discuss the method used in the research investigation. To a quire, the aim of the study researcher used the mono method, qualitative to collect the primary data through semistructured interviews. A research approach is a deductive approach that depends on a literature review of previous studies. This researcher built on the survey strategy through interviews with investors, creators, and specialists in blockchain technology which drives NFT, Metaverse, and Cryptocurrency. The research time horizon across-sectional study, the study focuses on the nature of NFT. Moreover, investigate the factors affecting risk and return for the following NFT, Metaverse, and cryptocurrencies. Also, the link between NFT, IP, Metaverse, and cryptocurrency. Furthermore, the prevalence of non-fungible tokens in the Middle East. In addition, secondary data is from financial websites like Bloomberg, PWC, and Binance.

Interviewee questions

What is a non-fungible token? What is the challenge you face in entering the NFT world? What is the challenge you face in entering the Metaverse? What is the challenge you face in entering crypto? What is the relationship between IP and NFT? What is the relationship between NFT and Metaverse? What is the relationship between NFT and cryptocurrency What are the factors affecting NFT return? Metaverse return Cryptocurrency return What are the risk factors investors should take into consideration when investing in NFT? Metaverse cryptocurrency How does NFT change the investment world? Has NFT changed the investor's thoughts about investment and how? What is the right method that you used in terms of selecting the right NFT investment? what is the potential in taking NFT's place in the Middle East? How much NFT is growing in the Middle East? What is the earning percentage from investing in NFT?



4. Finding and discussion

This chapter will focus on the results from interviews and link them with researcher questions, literature review, and secondary data that supported this result. The analysis method used in this research is the coding technique.

NFT and its nature

The first and second participants said that NFT is the main drive of Metaverse it is the assets you use inside Metaverse. As digital assets under the same umbrella, they have distinct qualities that distinguish them." (Omariba 2021) However, it contradicts the theory of (BLAKE FINUCANE) that said it is a technological breakthrough.

What are the challenges you face in entering the NFT, Metaverse, and cryptocurrency world? NFT

The first challenge would be the technical learning curve knowing how to keep how to save your NFT first of all how to buy them. And some people who lost for example bought a large amount of Cryptocurrency or in NFT and lost the password. NFTs of the art market, a lot of people started to buy an N F. T. But didn't have any knowledge about the art market. So, I still, need to gain knowledge about how it works to buy a piece of art. But the art market it's one example. Even NFTs are the game in the art of music and potential future in this people need to understand the industry first before buying an NFTS like they need to understand what they are buying. So, the challenge for the investors is to look at the best projects that represent those NFTs. Hidden creator. And mostly now the N F Ts are driven by hype and that means it's driven by just the talk of the people some of those N F Ts. Don't have any value at all. Do not accept these things easily. Do not accept new ideas. So, it's a challenge because the problem on it when opening a non-custodial wallet so you own the wallets. Will have 12, 18, or 24 passwords.so, if it loses these phrases it loses property or NFT bought from the market.

Ethereum Blockchain. will face a high gas fee sometimes Like art, and NFT projects the price of the art is \$100 or \$200. So, what is famous and known all the big artists are going to Ethereum Blockchain.

Metaverse

The same thing applies, when you talked about the N F T s because now, the main driver of those Metaverses is the N F T s that will be used inside the Metaverse because as a Metaverse can make a centralized and it's not a problem with that to make it a decentralized Metaverse, need to sell



spots of that Metaverse or rent it or give it to other people so they can utilize it, would do that by the use of those NFTs. So, the owner of that plot is an owner of an N F T. That will be used to rent or to build on it or to showcase a product or store inside of your Metaverse. And it probably could appear this one challenge in Metaverse. The challenge investors face in entering the Metaverse is which Metaverse platform they need, What do you want to achieve with that Metaverse platform? Do you need a Metaverse platform or not? Furthermore, what type of platform do you want to go on?

Cryptocurrencies

Ellen Doug coin means it does pump and people enter it and it dumps the people they enter it their investment has been 10 dollars from 1,000 to 10. On the other hand, this one challenge and might co-tome a coin like Shiba. Shiba is a mean coin who enter at the beginning there is a story about a person who invested in it 8,000 it went all the way to more than a billion dollars. This result is consistent with the theory say that "The risk of cryptocurrencies is high volatility, so it's too risky to invest in one currency" (By bit Learn). Wide market challenges cryptocurrencies now we have more than 20,000 kinds of coins. So as mentioned above education and knowledge is the first challenges investors face in entering the NFT world.

What is the relationship between IP and NFT?

Let's say that NFTs. Are the stump that can guarantee your intellectual property. That's the thing about NFTs. It's the only proof that will give you the flexibility to move from one place to another in the digital world. I mean I can show you that I have this IP number blah blah blah and this the property that I own and it's registered in this entity or that entity. But I can also forge that and it will discover that it's a forged document with NFTs. I mean the proof is instant. NFT can present a challenge for intellectual properties. I mean let's say I'm an artist I wrote, I painted the picture and then somebody else took my picture and sold it as an NFT. NFTS are stolen art. So, they are infringing on the intellectual property of the owner. But on the other hand, let's say I am an artist and I pay (Mike myself I convert my painting into an NFT. If I sell it in this case, we will not have an intellectual property issue. So, one of the challenges for intellectual property for NFT. But then I realized that he's told me he or she stole this art form, he took a picture of someone else's intellectual property. So, these are some complicated areas that intellectual property that can present challenges in the NFT. Let's say for example intellectual property is the concept of owning the intellectual concept of something and then you can have a patent. The thing is like from a



technology standpoint it proves it, but from a legal standpoint, it does not yet. Can it be accepted as legal proof? Do an NFT And he does not have an IP It means he stole it. It's a big problem for the project.

What is the relationship between NFT and Metaverse?

Now, the way we experience these assets is through a two-to-demand base which is the laptop, or a two-dimensional platform, which is the laptop. The Metaverse platform, let's see okay going to earn don't know certain attributes. Is going to prove that it's yours. So, it's proof of ownership but because it's So, blockchain it means that can prove it directly inside the metal gloves and can prove it also outside. And then after that on top of it, you can transfer these NFTs into other platforms where you can do more stuff. NFT let's say it's the technology. It's a technology as a digital asset. when going into the Metaverse and buying land to prove that the ownership of this land is by NFT. The NFT technology guarantees ownership inside or outside the Metaverse.

What is the relationship between NFT and cryptocurrency?

I don't see a relationship between Cryptocurrency and then there are different entities inside the Blockchain. I don't see any relation with it. There are 11 applications of Blockchain. NFT.s A third application of Blockchain is Ritterbusch a communication platform. So, The Blockchain a technology that empowers Bitcoin, also empowers N. Cryptocurrency is based on what call a year C20 standard tokens. thus, this token is fungible. It means that can create 10,000 tokens with the same characters. T. is a non-fungible token. So, which means that each token that going to be released is going to be unique. NFTS. Let's say based on the collection that does the NFT. Each one of the 10,000 is going to have different characters if it's going to be coded and it's going to make it So, it's not fungible. So that's the difference between the two and both of them are digital assets under the umbrella of blockchain. This consists with (Conti and Schmidt) said that Cryptocurrency is fungible while NFT is non-fungible and both are derived by blockchain." a token. let's say Sandbox has a coin called Jan So it's a token. It's the same Now you have NFT and when you go to Metaverse. earn tokens inside the Metaverse world. And when you earn tokens, that's called cryptocurrency.

What are the factors affecting NFT, Metaverse, and cryptocurrency return?

NFTs

Now, the way we experience these assets is through a two-to-demand base which is the laptop, or a two-dimensional platform, which is the laptop. The Metaverse platform, let's see okay going to



earn don't know certain attributes. Is going to prove that it's yours. So, it's proof of ownership but because it's So, blockchain it means that can prove it directly inside the metal gloves and can prove it also outside. And then after that on top of it, you can transfer these NFTs into other platforms where you can do more stuff. NFT let's say it's the technology. It's a technology as a digital asset. when going into the Metaverse and buying land to prove that the ownership of this land is by NFT. The NFT technology guarantees ownership inside or outside the Metaverse.

Metaverse

The people behind it are basically that for all of them. it's a project that needs people. sandbox why do people love it, because I can buy land, I can build a virtual building and I can do an academy through Metaverse and people pay me money to join my Metaverse Academy, this one thing. Another thing I can build again is the sandbox and if it's a good game people will come and they want to play it, and they would pay me money to play it. Just I can buy land, and make a party a virtual party in it. if the Metaverse, allows me to do all these things, we love it right?

Cryptocurrencies

Putting money in a savings account with the bank, the interest rate is about like 1% or even less because the bank is being, there is a lot of old computer system that we need to pay for and like the charges, a lot of fees and maintaining your bank is very expensive. If you go to a decentralized exchange or a Cryptocurrency platform in general, you can save your money, You're saving accounts in crypto and you're going to make 5-7% rather than 1% use like everything is automated. So, you can invest in Bitcoin and Ethereum at the same time with a single click and then you get the best performance of both. You can do what we call yield farming, meaning that you're going to go on a platform and that platform is going to automatically check for you the best rate all around in the system without any commercial incentive because it's all programming the smart contract. meaning that it has to find you the best rate. As a result, your return on investment in terms of Cryptocurrency, especially in decentralized finance. The classical finance world like banks, central banks, and financial institutions are looking at Blockchain technology today because it's cheaper to create money and make it to calculate and create products around it than we should take advantage of it. BNB it's a deflationary coin meaning the transactions that happened there fee played a part in these fees getting burned so the currency number did not increase but it decreased and this attracts investors There are coins that have 10 billion from it. They will put their money in this coin. Projects should be supported by Big VCs. As well as it must also have many



transactions on the chain so it can get supported and enter to exchange. A chance to enter a tierone exchange because it's a very important thing. The investor should look for projects that have a community as well because without the community the project will lose, accordingly, investors will lose the money invested in such a project.

What are the risk factors investors should take into consideration when investing in NFT, Metaverse, and cryptocurrency?

I think it's the same thing when it comes to the risk factors and investing in NFT. So, it means the same thing in the world that we have today, sometimes you can receive emails dressed in certain token cryptocurrencies and stuff like that, but they are fake and these people just want to take your personal information to empty your wallet or to try to hack you. Still, people are learning how to be careful about scams, and the currency well, so I think this is something that, that is a risk as well but to mitigate that for a couple of things. And then the second thing is you go on a platform like a clubhouse Twitter or discards and you try to check all the crypto communities and you can start to see like all the like the scam conversations or even on Reddit and stuff and you can learn about the patterns.

Don't start with money, you can't afford to lose This advice is repeated a lot but it's it's a fact start with \$500. That's you might lose everything if you did not do risk management if you did not manage your portfolio. However, they contain a lot of risks. That's you might lose everything if you did not do risk management if you did not manage your portfolio. You can easily lose everything. This consists of the theory that said NFTs give high returns. However, they contain a lot of risks. (Business Management) Another theory is that the risk of cryptocurrencies is high volatility, so it's too risky to invest in one currency. Software hacking and difficulty in transferring money. (By bit Learn)

How does NFT change the investment world?

It's natural for the people or the greed of the people will just let them flow into that market but it should stabilize sone the NFT. So, in terms of transferring assets, it's going to be way simpler for investors to do these things today. It's not how technology. I can I mean that building into the Blockchain through the NFT technology and fractionated and make it a fractionated. And I can rent out the apartment through that NFT so you can come and take one fraction and pay me through the smart contract. If you want to invest in let's, Say stock market, right? Can everyone invest in



the business stock market? Escalate the cycle of normal business. The cycle of So, the normal businesses which take 5–6 years here.

Has NFT changed the investor's thoughts about investment and how?

It recruits a lot of younger people, especially kids. I know like I hear here and their kids and they're familiar with it and they started to collect it even though their parents or their older siblings, have no clue what is Cryptocurrency or Blockchain. But this gets started it became part of the world. I think it brought two categories of people. I think it brought people who are coming from the classical world and now they are starting to invest in NFT. people born with the internet, they understand the game, they are like I don't know 15, 16 up to like 30 years old and they come and they invest directly on these platforms. They already have integrated that Blockchain technology is something that works and they are making investment out of it. I mean it was very difficult to do uh in the classic world today, it's very easy or let's say for example, you don't have enough money to buy a full painting but with a group of friends or you decided to build a decentralized autonomous organization, raise funds and try to dive at painting and factionalist today, it's very easy to do from a tax standpoint. I think this is what the NFT has brought up. I'm the guy, and I can sell land in whatever country, and someone like the land so he buys it through NFT.

What is the right method that you used in terms of selecting the right NFT investment?

Like at the projects, hype, and the roadmap after that the community and the people are behind it. Go to socials, see the followers, see what the people are saying, read articles, and do some digging and study the project before you put your money, On the other hand, look at the project that you know. AS well as the utility that the benefit investor will get from investing in this project. Also, Education: make sure that you are buying an NFT. So, you need to educate yourself and make sure you know how to set up a crypto wallet. It's in the ecosystem at the moment to try to get information about where to buy, and where to invest in everything. The important thing is the Branding, for the NFT Project.

Potentials of NFTs take place in the Middle East

Before you look into adopting cryptocurrencies and adopting if you look at the markets in the Middle East, it's very premature. Also, nobody is trying to educate themselves about the Blockchain so the Middle East will be years behind. Moreover, if you look at the Arabic content you will not learn anything if you want to learn, you have to look at the English side of it and that is, and that is a drawback for the Middle East. When looking at the demography of a country like



Saudi Arabia believe if my stats are correct 70% of the population is under 35 years old. We are talking to some people in Saudi Arabia in the Middle East region at the moment about an N.F.T. There is an interest, and interest is huge.

Growing of NFTs in the Middle East

Also, we started to see some projects in the Middle East, most of them in Dubai. While, (Trista Hamid) says "NFTs become a trend in the Middle East, where artists like Kristel Bechara and Aya Tarek have launched their own NFT projects. Now, Art Dubai, the region's largest art festival, is dedicating an entire area to digital art and NFTs." As well as one participant attended Dubai's largest art festival and said "Me and my friend were the only Arabs. No Arab so it's an opportunity.

What is the earning percentage from investing in NFT?

This depends on the project itself and the community behind the project. It is supply and demand so if the creator was active and always developing his project. People will like the projects and start using gaming if it's a game or collecting if it's an art. As a result of high demand, the earning percentage will go up. Therefore, we found projects give 10% return and others give more than 1000%.

5. Conclusions and recommendation

5.1. Conclusions

In conclusion, investors should choose carefully the projects they will invest in whether it is NFT, Metaverse, or Cryptocurrency. Take into consideration the nature of each one of them and the factors that affect risk and return. All of them are derived through blockchain technology. And since it is a new technology it contains high risk, high volatility, and a lot of scams. because it is not legally controlled so it is a higher risk than classic financial investment which is become a safe and stable market.

NFT is not a breakthrough technology it's a digital proof of ownership whether it is assets, currency, or commodities.

NFTs relation with IP, Metaverse & Cryptocurrency. NFTs are stumper tools, instant and digital proof that can guarantee intellectual property. Also, it is the main driver for the Metaverse. The main utility that will be used in the Metaverse and digital proof of owning anything inside the Metaverse. Besides, there is no relation between NFT and Cryptocurrency unless they are both inside the blockchain.



There is a huge potential for NFTs taking place in the Middle East, but still in the beginning. It is premature and needs a lot of education so they can create higher-quality projects. On the other hand, some big names started entering the NFT world like MBC Groupe and Elie Saab.

5.2. Recommendation

It is recommended investors and creators educate themselves about blockchain technology first then about NFT, Metaverse, and Cryptocurrencies to have a full understanding before investing. All investors choose the right project to invest in through careful analysis. And not only by following the hype. Creators of the project be honest clear and active in building a strong community for their projects. Because a strong community helps in the success of the project. Stockholders diversify their investments to reduce risk. Moreover, investing in NFT, Metaverse, and Cryptocurrencies as well as the stock market and Gold. Also, I recommend investors choose trust trading platforms. Also, advise business owners to start benefiting from blockchain technology as it is the future. As well as blockchain technology also gives high returns with lower costs.

6. Acknowledgments

I would like to thank my parents for all the love and support they have provided me over the years. They have been with me every step of the way, through the good and bad. I appreciate all their guidance and words of wisdom, which I will hold very near and dear to my heart.

I would like to sincerely thank my academic supervisor, Dr. Mohammed Binkhamis, for his guidance and support throughout the course. He was always there to help answer questions and guide me in finalizing my report. Finally, thank you to everyone who took part in my self-growth and helped me get through university and in completing my Master's Degree.

7. References

- Acello, R. (2021). Nonfungible tokens are all the rage now. What are they, and what should buyers watch for? Last modified October 1,. Accessed February 28, 2022. https://www.abajournal.com/magazine/article/nonfungible-tokens-are-all-the-rage-nowwhat-are-they-and-what-should-buyers-watch-for
- Bloomberg Intelligence. (2021). Metaverse may be an \$800 billion market, the next tech platform. Last Modified December 01,. Accessed May 6, 2022.


https://www.bloomberg.com/professional/blog/Metaverse-may-be-800-billion-market-next-tech-platform/.

- Chintalapoodi, P. (2021). Are non-fungible tokens (NFT) intellectual property? Last Modified March 22. Accessed February 26, 2022. https://www.chiplawgroup.com/are-nftsintellectual-property/.
- Conti, R., and J. Schmidt. (2022). What is an NFT? How Do NFTs Work?. Last Modified Sep 16. Accessed Apr 30, 2022. https://www.forbes.com/advisor/in/investing/cryptocurrency/what-is-an-nft-how-do-nftswork/
- Cudd, M., K. Ritterbush, M. Eduardo, and C. Smith. (2018). Cryptocurrency Returns. In *Blockchain and Cryptocurrencies*, ed. Asma Salman and Muthanna G. Abdul Razzaq, 1–13. Online publication: Intechopen.
- Dalton, J., and L. Liu. Seeing is believing: PwC. Last modified (2019). Accessed Mar 30, 2022. https://www.pwc.com/gx/en/industries/technology/publications/economic-impact-of-vrar.html
- Deepika, R. and R. Dileep. (2022). NFTs and their relationship with IP rights—IPLF. Last modified November 19, 2021. Accessed on May 26, 2022. https://www.ipandlegalfilings.com/nfts-and-its-relationship-with-ip-rights/.
- Finucane, B. (2021). The NFT boom: A technological breakthrough on the blockchain that revolutionizes digital ownership for art, collectibles, and gaming. Last Modified March 1, 2021. Accessed April 30, 2022. https://financial-news-now.com/the-nft-boom-atechnological-breakthrough-on-the-blockchain-that-revolutionizes-digital-ownership-forart-collectibles-and-gaming/.
- Hamid, T. (2022). How have NFTs impacted the Middle East's art world? Last modified March3. Accessed April 26, 2022. https://www.wamda.com/2022/03/nfts-impacted-middle-eastsart-world.
- Takyar, A. Metaverse and its link with NFTs. Accessed on 26 May 2022. https://www.leewayhertz.com/Metaverse-andnfts/#:~:text=NFTs%20work%20in%20the%20Metaverse%20as%20realworld%20objects,NFTs%20and%20Metaverse%20to%20utilize%20their%20combined%2 0benefits



- Unlock Blockchain. Saudi MBC group to launch NFT collectibles. Last modified March 3, 2022. Accessed on May 27, 2022. https://www.unlock-bc.com/saudi-mbc-group-to-launch-nft-collectibles
- Omariba, Is NFT A Cryptocurrency? (Beginner's Guide). Last modified November 25, 2021. Accessed Mar 27, 2022.https://coinwut.com/nft-cryptocurrency/

Copyright © 2023 Bodour Idris Radwan, Dr. Mohammed Binkhamis, AJRSP. This is an Open-Access Article Distributed under the Terms of the Creative Commons Attribution License (CC BY NC)

Doi: https://doi.org/10.52132/Ajrsp.e.2023.54.2



Detection of Pneumonia from Chest X-ray Images Using Transfer Learning and Ensemble Learning

Bahatheq Tariq Ahmed S¹, Jayanth Balasubramanian², Koh Shang Hui³

Undergraduate, Computer Science, National University of Singapore, Singapore ^{1,2,3}

Email: <u>Tariqbahatheq@outlook.com</u>

https://colab.research.google.com/drive/1YGE9p2B4Fgx5dN2omxA0wa4djPkZigpI?usp=sh aring

Abstract

Pneumonia, characterized by lung inflammation and caused by various strains of bacteria and viruses, consistently ranks as one of the top three causes of death in Singapore. Despite chest X-ray being the standard imaging test for pneumonia, its diagnostic accuracy has limitations due to factors like low specificity and subjective variance among radiographers. This research aims to enhance the diagnosis by predicting pneumonia based on chest X-ray images sourced from a Kaggle dataset with 5856 images, primarily from pediatric patients at the Guangzhou Women and Children's Medical Center. A novel approach modifies the Kaggle data split to introduce more validation data and employs data augmentation techniques such as random flips and rotations to stabilize the model. Convolutional Neural Networks (CNNs) form the core of the prediction methodology. Simple CNNs are evaluated, followed by transfer learning models using ImageNet architectures. The models are assessed based on their weighted F1 scores, with a special emphasis on recall to ensure critical cases aren't missed. Ensemble techniques, such as voting, are explored to further enhance prediction capabilities and robustness. The paper culminates by comparing these models against existing frameworks and provides insights into their potential application in real-world medical diagnostics to further enhance the medical field.

Keywords: AI, Machine learning, Deep Learning, Neural Networks, Convolutional Neural Networks, Transfer learning, Ensemble models, Explainable AI, Classification, Pneumonia, AI & Medicine



1. Introduction:

Pneumonia is an inflammatory condition affecting the lungs, predominantly the tiny air sacs known as alveoli. Typically, these sacs fill with pus or fluid, making breathing painful and limiting oxygen intake. Caused by a plethora of bacteria, viruses, and even fungi, pneumonia presents a significant healthcare challenge globally.

In Singapore, the gravity of this disease is further underscored, ranking consistently among the nation's top causes of death. Traditional diagnostic methods, such as chest radiography, have been employed as the frontline defense to detect this ailment. However, the accuracy of these methods is often marred by various challenges, ranging from the inherent limitations of the imaging technique to the subjective interpretations of the radiographers.

Amidst these challenges, the advent of artificial intelligence and machine learning offers a beacon of hope. By leveraging vast datasets and intricate algorithms, researchers are continuously striving to improve the accuracy and speed of pneumonia diagnosis. This paper delves into one such endeavor, exploring the potential of convolutional neural networks and ensemble learning to detect pneumonia from chest X-ray images. Through a nuanced exploration of methodologies, datasets, and evaluation criteria, this research aims to contribute to the ongoing efforts in combating this formidable disease.

Motivation

Pneumonia consistently ranks among the top 3 principal causes of death in Singapore, as reported by the Ministry of Health. It is characterized by lung inflammation, particularly in the air sacs, and is caused by various strains of bacteria and viruses.

A chest radiography, or chest X-ray, is the standard imaging test for pneumonia. However, it has been noted that the diagnostic accuracy of chest radiography is limited (Self et al. 2013, van den Berk et al. 2022). One reason is its low specificity (Esayag et al. 2010). Additionally, subjective variance among radiographers induces significant uncertainty in chest radiography reports, further complicating clinical diagnoses.

Comparatively, a computed tomography (CT) scan displays slightly better sensitivity and significantly higher specificity. A CT scan is often employed to rule out harder-to-detect cases of pneumonia. However, it remains prohibitively expensive to be used as a first-line test. Thus, an



accurate automated computer-aided diagnosis system using chest X-ray images has both medical and economic benefits.

Dataset

The chest X-ray images used are from a Kaggle challenge, and they are sourced from research done by Kermany in 2018. 5856 images consisting of 4273 positive 'pneumonia' and 1583 negative 'normal' samples were selected from one to five years old pediatric patients at the Guangzhou Women and Children's Medical Center, Guangzhou.

The Kaggle data split was modified to introduce more validation data. 20% of the testing dataset was randomly split and used to supplement the small validation dataset. A fixed seed was used for this split to ensure consistency across all trained models and to facilitate comparison between them. The decision to split the validation set from the testing set was motivated by an observation that the training and testing sets were dissimilar, complicating early attempts at model selection. After the split, more consistency between validation and testing was achieved.

Г

Split\ Label	Normal	Pneumonia	Total
Train	1341	3875	5216
Validation	8	8	16
Test	234	390	624
Total	1583	4273	5856

Split\ Label	Normal	Pneumonia	Total
Train	1341	3875	5216
Validation	60	81	141
Test	182	317	499
Total	1583	4273	5856

Figure 1: Structure of the Kaggle dataset

Figure 2: Structure of the modified Kaggle dataset

Weighted random sampling was applied for the training dataset to account for label imbalances. As before, a generator with a fixed seed was used to ensure uniform training conditions for all models.

The following transformations were applied to the images: resizing, normalization with respect to the mean and standard deviation of the unaugmented training dataset, and a 80% center crop. The center crop removes large empty spaces and focuses on the lungs.







Augmentation

To make the model more stable and less prone to noise, new data was generated by augmenting the current data. This was also done to make up for the amount of data we have. The following transformations were applied to the images: random horizontal flip, random rotation, and random brightness change.

Strategy

Batch gradient descent was employed to train all the networks, with a typical batch size of 48 to 64. To speed up convergence, AdamW was used to adapt the per-parameter learning rate. The models' accuracies on the validation dataset were calculated after each epoch. Early stopping was implemented to prevent model overfitting by stopping training if validation accuracy dropped by more than a threshold of 0.1 (which worked best in our testing) over 3 consecutive epochs.

Various learning rate schedulers were employed to adjust the learning rate based on validation accuracy. For ResNet based models, ReduceLROnPlateau was found to work best. This required some fine-tuning: for example, one combination of schedulers given as an example on the PyTorch docs, ExponentialLR followed by MultiStepLR, was found to make the accuracy of the trained Resnet based model worse. Other models were trained using StepLR to reduce the learning rate after a fixed number of iterations.

Evaluating the Models

Many criteria were considered to be used as the basis for choosing the best models. The first option was to choose recall. If the model is used as a diagnostic aid for medical workers, missing a pneumonia case can be critical. The next option was to use accuracy, the most straightforward option given that the dataset was balanced using weighted random sampling. Moreover, it is transparent for workers in the medical field and is widely used in that field. Another option was



precision, or the positive predictive value. For such a model, a positive prediction is most likely to be an actual positive. A potential drawback might be a larger proportion of false negatives.

We reason that solely relying on recall or precision alone is inadequate for this computer-aided diagnosis as the other scores can be very low. A weighted F1 score focused more on recall was chosen. We prefer recall because, for this critical disease, we prefer that the model doesn't miss any cases and classifies them as negative. The beta value chosen in this case is 2.

$$F_{\beta} = (1 + \beta^2) \cdot \frac{precision \cdot recall}{(\beta^2 \cdot precision) + recall}$$

Baseline CNN

To provide a baseline accuracy with which to compare later models with, a basic deep CNN was trained using the following architecture:

Convolution layers:

 $Conv (3, 32) \rightarrow ReLU \rightarrow BN(32) \rightarrow maxpool(2, 2) \rightarrow Conv(32, 64) \rightarrow ReLU \rightarrow Dropout(0.1) \rightarrow BN (64) \rightarrow maxpool(2, 2) \rightarrow Conv(64, 64) \rightarrow ReLU \rightarrow BN(64) \rightarrow maxpool(2, 2) \rightarrow Conv (64, 128) \rightarrow ReLU \rightarrow Dropout(0.2) \rightarrow BN(128) \rightarrow maxpool(2, 2) \rightarrow Conv (64, 128) \rightarrow ReLU \rightarrow Dropout(0.2) \rightarrow BN(128) \rightarrow maxpool(2, 2) \rightarrow Conv (64, 128) \rightarrow ReLU \rightarrow Dropout(0.2) \rightarrow BN(128) \rightarrow maxpool(2, 2) \rightarrow Conv (64, 128) \rightarrow ReLU \rightarrow Dropout(0.2) \rightarrow BN(128) \rightarrow maxpool(2, 2) \rightarrow Conv (64, 128) \rightarrow ReLU \rightarrow Dropout(0.2) \rightarrow Dropout(0.2)$

Conv (128, 256) \rightarrow ReLU \rightarrow Dropout(0.2) \rightarrow BN(256) \rightarrow maxpool(2, 2)

Classifier:

Linear (9216, 128) \rightarrow ReLU \rightarrow Dropout(0.2) \rightarrow Linear(128, 2)

Training Parameters:

	Figure 4: Architecture for the baseline CNN
Epochs	: 20
Scheduler	: StepLR - size 7, gamma 0.1
Loss Function	n: CrossEntropyLoss
Learning rate	: 0.00001
Optimizer	: AdamW
Kernel size	: 3

Transfer Learning

From 2012 to 2017, increasingly deeper CNN architectures showed drastic improvements in the ImageNet Large Scale Visual Recognition Challenge (ILSVRC).



The availability of a dataset of over 1.2 million training images, orders of magnitude above past datasets, was a key factor in enabling the training of larger yet more accurate models.

A direct application of top-performing ILSVRC models to the Kaggle dataset is likely to result in model overfitting as the dataset provides only 5216 training images. Instead, an inductive transfer learning was used to leverage existing ConvNet architectures. By replacing only the classifier layers, the hypothesis space of possible models is restricted beneficially.

In total, 7 classifiers were adapted for transfer learning: AlexNet, InceptionNetV3, EfficientNetV2, DenseNet121, GoogLeNet, ResNet50, and VGG19BN. For all models, the final classifier layer was replaced with a three-layer classifier as described in Figure 5. The parameter n was varied to match the output size of the previous layers. k = 128 or 256 and d was varied in pursuit of higher accuracy. The model parameters in all other layers were frozen.

Classifier:

Linear(n, 512) \rightarrow ReLU \rightarrow Dropout(d) \rightarrow Linear(512,k) \rightarrow ReLU \rightarrow Linear(k,2)

Training Parameters:

Optimizer : Adam/AdamW Learning rate : 0.00001 for AdamW, 0.001 for Adam Loss Function: CrossEntropyLoss Scheduler : StepLR - size 7, gamma 0.1/ ReduceLROnPlateau Epochs : 20 EarlyStopper : patience 3, delta 0.1

Figure 5: Classifier architecture and model parameters used for transfer learning

Frequency Domain Learning

Xu et al. noted that existing structures of notable neural networks can be leveraged to perform deep learning in the frequency domain. An exploration of these ideas was performed by analyzing an instance of transfer learning on the frequency space. After a 2D FFT, the modulus of the real and complex parts was taken. The frequency image was then resized to 512x512 and normalized to a mean of 0 and standard deviation of 1. Transfer learning was then conducted using VGG19BN with the classifier and parameters described in Figure 5.



2. Discussion and Analysis

Architecture	Overall Accuracy	Precision	Recall	Weighted F1
Baseline CNN	76.95	73.60	99.37	92.87
Fourier VGG	89.38	89.31	96.53	94.99
AlexNet	91.78	90.12	97.79	96.15
InceptionNetV3	80.76	77.56	98.11	93.17
EfficientNetV2	91.58	91.79	95.27	94.55
DenseNet121	89.78	88.00	97.16	95.18
GoogleNet	89.38	88.82	95.27	93.91
ResNet50	91.58	90.56	96.85	95.52
VGG19BN	90.18	90.12	94.95	93.94

The accuracy, precision and recall of the models tested are shown in Figure 6.

Figure 6: Accuracy, precision, recall, and weighted F1 score (β =2) of different ML models in %

All models tested showed excellent recall with very few false negative identifications. Precision was less noteworthy, with a significant false positive rate. In contrast, there were near-zero false negative identifications.

With the exception of InceptionNetV3, the transfer learning models substantially outperformed the baseline CNN in terms of accuracy. The Fourier VGG model trained on the frequency space was competitive with the traditional transfer learning models.

Evaluating our model against other state-of-the-art models can provide insights into its competence and resource utilization. On Kaggle, the source of our dataset, most models achieve a testing accuracy between 85 and 90%. However, two models outperform the rest. The first is a CNN trained from scratch, achieving 92.63% accuracy (Mathur, 2020). The second employs a fine-tuned ResNet152 model, attaining 91.99% accuracy (Barbosa, 2022).



Our best-performing model achieved 91.78% accuracy, placing it among the top-performing models for this specific dataset. On the other hand, in 2022, Li and Li demonstrated a 99.62% accuracy using ensemble methodologies for COVID-19 pneumonia detection on a separate dataset. As a result, our model may not be suitable for deployment in the medical field as a standalone diagnostic tool. Instead, it could be used to assist radiologists in their decision-making process, rather than serving as the sole determinant.

Explaining Model Outputs

With deep learning models becoming increasingly deep (even the baseline CNN has 26 layer) and complex, such as with skip connections between layers, they become even more opaque in their decision making. The tens or even hundreds of thousands of parameters seemingly renders these networks to be all but a black box classifier. Two problems naturally arise: (1) difficulty in trusting the model's outputs (2) difficulty in monitoring and debugging the model.

In this section, feature (pixel) attribution is examined. Each pixel's contribution to the model's classification, a weaker but useful notion of explainability, is calculated. Formally, given a complex model f and an input instance (image) x, one aims to

- Map x to the simplified input x' through the mapping function h: h(x') = x (In our case, since the input instance is an image, a sample mapping function h could map a vector of 0s and 1s indicating the presence or absence of a group of pixels to an image (where 0 means that "superpixel" is replaced with the average RGB value of its neighbors).
- Create a simplified model g such that g(z') ≈ f(h(z')) ∀ z' ≈ x'. (Lundberg, Lee 2017) LIME, an additive explanation model, is utilized. It assigns a contribution φ_i to each simplified feature z_i' ∈ z' (where z has M dimensions) such that g(z') = φ₀ + Σ^M_{i=1} φ_iz'_i ∀ z' ≈ x'

LIME uses penalized linear regression to minimize Least Squared Loss between f(h(z')) and g(z'), ensuring that g is faithful to the original model f around the given input instance (Lundberg, Lee 2017). Figures 7 and 8 show the outputs from running LimeImageExplainer on two of our best models, and ResNet50 and EfficientNet.





Figure 7: Chest X-Ray of a person with pneumonia. Left: yellow boundary indicates the top 5 features that cause the trained ResNet50 model to classify the image as "Pneumonia". Right: green and red regions indicate features that contributed positively (and negatively, respectively) towards "pneumonia" classification



Figure 8: Chest X-Ray of a person with pneumonia. Left: yellow boundary indicates the top 5 features that cause the trained EfficientNet model to classify the image as "Pneumonia". Right: green and red regions indicate features that contributed positively (and negatively, respectively) towards "pneumonia" classification

Despite the identical positive classification, the two models pay attention to different regions to make the classification. Comparing the yellow boundaries in Figure 7 and 8, we can see that the top and middle of the left lung contributed positively to classification as Pneumonia for both models. However, if we compare the red and green regions for the two models, we notice that the models disagree on the contribution of the bottom right of the lung (contributes positively to EfficientNet classification, negatively to ResNet classification). Unfortunately, our team does not have the medical expertise to determine which model is correct regarding this.

From the above discussion, it is clear that pixel attribution using tools like LIME can give more information to a doctor than a binary classification to help a doctor reach an informed conclusion. However, disagreement between the different models suggests that the information could potentially be misleading,



and a similar approach with LIME plots of multiple models could be used by the doctor to find common regions that both models found significant in making a prediction.

Voting Ensembles

The training of multiple independent deep learning models motivates the use of ensemble learning methodologies. A combination of multiple hypotheses may produce higher accuracy than any individual constituent hypothesis.

Bayes classifiers in the form of unweighted voting ensembles were tested first using all 7 trained transfer learning models and next using the top 5 models by weighted F1 score. In light of the significant false positive rate of the transfer learning models, three levels of bias were evaluated. The first, an unbiased voting, was a simple majority algorithm requiring 4 of 7 or 3 of 5 votes. The second required one additional positive vote while the third required two more (effectively a unanimous decision for the ensemble of 5) for an overall positive classification respectively. The stricter requirements for an overall positive result represent an increasing negative bias, or bias towards the negative or 'normal' classification. The results are shown in Figures 10 and 11.

We observe a positive trend in the precision and negative trend in recall as the negative bias increases. This is a result of a decreasing false positive but increasing false negative rate. The unbiased, simple majority ensemble was the best performing ensemble. However, it did not improve upon AlexNet, the best performing transfer learning model. This indicated a high degree of similarity between the transfer learning models.

Ensemble	Overall Accuracy	Precision	Recall	Weighted F1
Simple Majority	91.78	90.35	97.48	95.97
5 or more	92.79	93.00	95.90	95.31
6 or more	92.38	94.86	93.95	94.13

Figure 9: Accuracy, precision, recall and weighted F1 score (β=2) for the unweighted voting ensembles using 7 models in %



Ensemble	Overall Accuracy	Precision	Recall	Weighted F1
Simple Majority	91.98	91.10	96.85	95.64
4 or more	92.18	93.71	93.86	93.83
Unanimous	87.37	95.68	89.41	90.60

Figure 10: Accuracy, precision, recall and weighted F1 score (β =2) for the unweighted voting ensembles using 5 best-performing models (by weighted F1 score) in %

3. Recommendations:

- 1. **Further Exploration of Transfer Learning**: Given the promising results observed from transfer learning, it is recommended to explore more recent architectures and fine-tuning techniques. This could enhance model performance and adaptability to varied datasets.
- 2. **Data Augmentation and Expansion**: To mitigate the risk of overfitting, especially when adapting large models to relatively smaller datasets, it would be beneficial to consider more advanced data augmentation techniques. Additionally, collaborations with medical institutions could provide a larger and more diverse dataset, further enhancing model robustness.
- 3. **Ensemble Learning**: The research demonstrated the potential of ensemble learning in boosting accuracy. Exploring different ensemble techniques, such as stacking or bagging, could potentially lead to even better results.
- 4. **Explainability and Trust**: As machine learning models become integral to medical diagnostics, ensuring their transparency and trustworthiness is crucial. Further research into model explainability, beyond pixel attribution, is recommended. This could enhance trust among medical professionals and facilitate the adoption of these tools in clinical settings.
- 5. **Collaboration with Radiologists**: The model, while promising, should not be viewed as a standalone diagnostic tool, given the current accuracy levels. Collaborations with radiologists could provide insights into practical challenges and needs, leading to models better tailored for real-world application.
- 6. **Frequency Domain Analysis**: The exploration into frequency domain learning showed potential. It's recommended to delve deeper into this area, perhaps looking at different transformation techniques or leveraging domain-specific knowledge



4. Conclusion and Future Work

Based on the weighted F1 scores from all the models and ensembles, AlexNet achieved the highest score.



Figure 11: Confusion matrix for AlexNet

Further classification of positive pneumonia cases by cause (bacterial or viral) can be explored. While the dataset explanation on Kaggle notes that a typical bacterial pneumonia exhibits a local anomaly in the chest X-ray and a viral pneumonia is characterized by diffuse patterns, it is difficult for an untrained eye to differentiate the two in practice.

Many new large models being deployed in 2022 and 2023 claim to be extremely efficient on data. These include the recently released and commercially available Amazon Titan foundation models. Training using such models can be explored to further enhance the results of the project at the expense of the project budget.

There is ample room for fitting other architectures from ILSVRC or elsewhere into the frequency space. In 2021, Han and Hong introduced specialized Fourier CNNs and experimented with shallow networks. Adapting their ideas to deeper networks may yield better results.

5. Ethical Consideration:

This research prioritizes the ethical standards integral to scientific endeavors, particularly in the realm of medical research. Herein, we outline the key ethical considerations that were adhered to:

- 1. **No Human Experiments**: At no point did this study involve direct experiments on humans by the authors. The research was fundamentally computational, focusing on the analysis of pre-existing datasets.
- 2. **Data Sources**: The data used in this research is sourced from a Kaggle challenge, which in turn was based on research done by Kermany in 2018. It's crucial to understand that all data



used was anonymized and void of any personal identifiers, ensuring the privacy and confidentiality of the patients from whom the X-ray images were derived.

- 3. **Patient Consent & Approvals**: While the authors did not directly conduct experiments or collect data, it's implicit that the original data collectors sought necessary consent from patients or their guardians, especially given the sensitive nature of medical imaging. Moreover, the necessary approvals from relevant authorities would have been secured by the primary data collectors.
- 4. **Protocols Followed**: The research strictly followed data handling and analysis protocols to ensure the integrity of the results. Furthermore, while the models and findings show promise, it's crucial to emphasize their supplementary role in medical diagnosis. Decisions based on these findings should be made with caution, ideally in tandem with expert human judgment.
- 5. **Transparency & Openness**: The research aims to contribute to the broader scientific community. As such, efforts have been made to ensure transparency in methodology, findings, and potential limitations. This open approach facilitates peer review and collective advancements in the field.

By adhering to these principles, this research aims to be both scientifically rigorous and ethically responsible, ensuring that advancements made contribute positively to patient care and the broader medical community.

6. References

- Bai, T.; Luo, J.; Zhao, J.; Wen, B.; Wang, Q. (2021). Recent Advances in Adversarial Training for Adversarial Robustness. arXiv:2102.01356.
- van den Berk, I. A. H.; Kanglie, M. M. N. P.; van Engelen, T. S. R. et al. (2022). Ultra-low-dose CT versus chest X-ray for patients suspected of pulmonary disease at the emergency department: a multicentre randomised clinical trial. *Thorax*. doi.org/10.1136/thoraxjnl-2021-218337
- Esayag, Y.; Nikitin, I.; Bar-Ziv, J.; Cytter, R.; Hadas-Halpern, I.; Zalut, T.; Yinnon, A. M.
 (2010). Diagnostic Value of Chest Radiographs in Bedridden Patients Suspected of Having Pneumonia. *The American Journal of Medicine*, *123*(1), 88.
 doi.org/10.1016/j.amjmed.2009.09.012



- Han, Y., Hong, B. (2021). Deep Learning Based on Fourier Convolutional Neural Networks Incorporating Random Kernels. *Electronics* 2021, *10*(16), 2004. doi.org/10.3390/electronics10162004.
- He, K., Zhang, X.; Ren, S.; Sun, J. (2015). Deep Residual Learning for Image Recognition. arXiv:1512.03385.
- Hosna, A.; Merry, E.; Gyalmo, J. et al (2022). Transfer learning: a friendly introduction. *J Big Data*, 9(102). doi.org/10.1186/s40537-022-00652-w.
- Huang, G.; Liu, Z.; van der Maaten, L.; Weinberger, K. Q. (2016). Densely Connected Convolutional Networks. arXiv:1608.06993.
- IBM. (2020). Adversarial Robustness Toolbox: One Year Later with v1.4. https://research.ibm.com/blog/adversarial-robustness-toolbox-one-year-later-with-v1-4. Accessed: 2023-04-18
- Kaggle. (2018). Chest X-Ray Images (Pneumonia). https://www.kaggle.com/datasets/paultimothymooney/chest-xray-pneumonia. Accessed: 2023 03-11.
- Kaggle. (2020). Pneumonia Detection using CNN(92.% Accuracy). https://www.kaggle.com/code/madz2000/pneumonia-detection-using-cnn-92-6-accuracy. Accessed: 2023-04-11.
- Kaggle. (2022). Chest X-Ray (Pneumonia) CNN & Transfer Learning. https://www.kaggle.com/code/jonaspalucibarbosa/chest-x-ray-pneumonia-cnn-transferlearning. Accessed: 2023-04-11.
- Krizhevsky, A.; Sutskever, I.; Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, 60(6), 84–90. doi.org/10.1145/3065386.
- Li, D., Li, S. (2022). An artificial intelligence deep learning platform achieves high diagnostic accuracy for Covid-19 pneumonia by reading chest X-ray images. *iScience*, 25(4). doi.org/10.1016/j.isci.2022.104031. arXiv:1705.07874.

Lundberg, S., Lee, S. (2017). A Unified Approach to Interpreting Model Predictions.



Ministry of Health Singapore. 2022. Principal Causes of Death. https://www.moh.gov.sg/resources-statistics/singapore-health-facts/principal-causes-ofdeath. Accessed: 2023-04-04.

- Self, W. H.; Courtney, D. M.; McNaughton, C. D.; Wunderink, R. G.; Kline, J. A. (2013). High discordance of chest x-ray and computed tomography for detection of pulmonary opacities in ED patients: implications for diagnosing pneumonia. *The American journal of emergency medicine*, 31(2), 401–405. doi.org/10.1016/j.ajem.2012.08.041
- Simonyan, K., Zisserman, A. (2014). Very Deep Convolutional Networks for Large-Scale Image Recognition. arXiv:1409.1556.
- Szegedy, C.; Liu, W.; Jia, Y.; Sermanet, P.; Reed, S.; Anguelov, D.; Erhan, D.; Vanhoucke, V.; Rabinovich, A. (2014). Going Deeper with Convolutions. arXiv:1409.4842.
- Tan, M., Le, Q. V. (2019). EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. arXiv:1905.11946.
- Xu, K; Qin, M.; Sun, F.; Wang, Y.; Chen, Y.; Ren, F. (2020). Learning in the Frequency Domain. arXiv:2002.12416

Team Member Roles

Tariq: Augmentation, GoogleNet, EfficientNet, AlexNet, Inceptionv3, SimpleCNN, DenseNet121, Evaluation, Meeting/Team coordination. Report: Augmentation, Baseline CNN, Evaluating the models, Discussion (part), Conclusion (part).

Jayanth: Wrote main training, validation and testing loops, SimpleCNN, EarlyStopper, ResNet-50, ResNet-34, LIME explainability, adversarial-robustness-toolbox for evasion attacks. Report: Strategy, Explaining model outputs, Improving model robustness

Shang Hui: VGG19BN, Fourier VGG, Unbiased and biased voting ensembles. Report: Abstract, Motivation, Dataset, Voting Ensembles, Conclusion (part), Frequency Domain Learning. Referencing and formatting.

Copyright © 2023 Bahatheq Tariq Ahmed S, Jayanth Balasubramanian, Koh Shang Hui, AJRSP. This is an Open-Access Article Distributed under the Terms of the Creative Commons Attribution License (CC BY NC)

Doi: https://doi.org/10.52132/Ajrsp.e.2023.54.3



Fractional partial Differential Equations for Laplace transformation Caputo-Fabrizo and Volterra integration

Dr. Mariam ALmahdi Mohammed Mulla

Department of Mathematics, University of Hafr AL-Batin (UHB) Hafr AL-Batin, KSA

ORCID: 0000-0001-9257-8237

Email: marimdx2014@gmail.com

Abstract:

In this paper we note the numerical methods for solving fractional differential equations, defined in the derivative of the Caputo-Fabrizio fractional operator and Laplace transform of fractional derivatives for integer order, solving differential equation problems using the Laplace transform method, and reducing to Volterra's integral equation, Laplace transform of the Mittage-Leffler function, this problem is not easy to solve analytically because an analytical solution is sometimes not available, even if an analytical solution is available, but it is complected, timeconsuming and expensive, so we need to develop a numerical method to address the relevant problem, Analyze a precise result such as the integral or exact expression of a solution to obtain a qualitative answer that shows us what is happening with each variable while numerical methods are more adaptable in the approximate result to obtain quantitative results by iteratively creating an approximate solution sequence for mathematical problems. The method will solve a non-homogeneous linear differential equation directly, following basic steps, without having to solve the integral equation and solutions separately and non-linear differential equations with the rational factor by developing analytical or numerical techniques to find approximate solutions. Finally, we studied some applications, especially for nonlinear differential equations with the rational operator.

Keywords: Laplacian Transform Interpretation, fractional Caputo–Fabrizio derivative operator, the Volterra Integral Equation, Existence and uniqueness, Iterative Laplace transform method.



1. Introduction

The mathematical models involving fractional derivatives were given noticeable importance because they are more accurate and realistic as compared to the classical order models [1,2]. Fractional differential equation, particularly fractional calculus equation and derivatives of functions gamma function while investigating the interpolation problem. There are several approaches leading to the definition of gamma function. However, this in Mathematics we are not looking at the usual integer order but at the non-integer order differential, and derivatives [3]. The Riemann-Liouville fractional differential operators have played a significant role in the development of the theory of differentiation and integration of arbitrary order, the Method of Volterra Integral Equation, Laplace transform of the Mittage–Leffler function, we introduced the series which converges to the solution of an initial-value to Volterra integral problem [4]. These are called fractional derivatives and fractional integrals, which can be of real or complex integer, and therefore also include integer orders. In this study, we refer if we are talking about the combination of these fractional derivatives has significant applications. Motivated by the advancement of fractional calculus, These differential equations involve several fractional differential operators like Riemann-Liouville, Caputo, [5], and modeling of materials and diffusion and expansion processes [6]. To avoid these problems, we find that the fractional partial differential operator has a substitution kernel with exponential decay [7]. Operator is best suited for modeling some classes as follows:

$$\begin{cases} D_{t_0}^{\alpha} y(t) \\ y(t_0) \end{cases}$$
(1)

To confirm the existence and uniqueness of the solution to problem (1) suppose that f(x, y). The function is continuous and fulfills Lipschitz's condition with respect to the second variable [8]. The initial value problem (1) can be transformed into an equivalent Volterra integral equation.

$$y(t) = y_0 + \frac{1}{\Gamma(\alpha)} \int_{t_0}^t (t - x)^{\alpha - 1} f(x, y(x)) dx$$
(2)



2. Definition of fractional calculus

We reviewed some definitions of the fractional partial derivative and the fractional integral. One should note that trigonometric functions of order n are generalizations of the sine and cosine functions of fractional calculus.

Definition 2.1 Fractional calculus is used for integrals and fractional partial derivatives [9]. It can be said that the order of numbers is truly arbitrary or even the order of a complex number. There are many definitions of the partial and integral derivation, such as we described. Other definitions can be found in [10,11]. Here we use D and I to denote the fractional derivative and the fractional integral, respectively.

Definition 2.2 It can be generalized that the integer-order classical partial derivation, which is used for continuous function f(t) is.

$$f^{(n)}(t) = \lim_{h \to 0} \frac{1}{h^2} \sum_{r=0}^{n} (-1)^i \binom{n}{i} f(t-ih),$$
(4)

Where $\binom{n}{r}$ is the binomial coefficients. If *n* is replaced by $\alpha \in \mathbb{R}$ we get

$$D_{\alpha,t}^{\alpha}f(t) = \lim_{h \to 0^{+}} \frac{1}{h^{\alpha}} \sum_{r=0}^{\frac{t-\alpha}{h}} (-1)^{i} {\alpha \choose i} f(t-ih),$$
(5)

where we denote the base function and the α denotes the starting point of the interval. **Definition 2.3** The Grünwald-Letnikov integral of arbitrary order is:

$$I_{\alpha,t}^{\alpha}f(t)\lim_{h\to 0^+}\frac{1}{h^{\alpha}}\sum_{r=0}^{\frac{t-\alpha}{h}}(-1)^i \binom{\alpha}{i}f(t-ih),$$
(6)

Definition 2.4 Riemann-Liouville. The α th order Riemann-Liouville derivative of function is.

$$D^{\alpha}_{\alpha,t}f(t) = \frac{1}{\Gamma(n-\alpha)} \frac{\partial^n}{\partial t^n} \int_{\alpha}^{t} \frac{f(x) \, dx}{(t-x)^{1-\alpha}},\tag{7}$$

And the integral

$$I_{\alpha,t}^{\alpha}f(t) = \frac{1}{\Gamma(\alpha)} \int_{\alpha}^{t} \frac{f(x) \, dx}{(t-x)^{1-\alpha}} \tag{8}$$



Definition 2.5 The Riemann-Liouville definition is important for the development of fractional derivatives, but it is difficult to calculate the integral with physically explicable elementary points. [12] Caputo solved this issue by creating a new definition.

$$D_{\alpha,t}^{\alpha}f(t) = \frac{1}{\Gamma(n-\alpha)} \int_{\alpha}^{t} (t-x)^{n-\alpha-1} \frac{\partial^{n}f(x)}{\partial x^{n}} dx, \quad n-1 < \alpha < n \quad (9)$$

3. Numerical and Analytical methods

There are different ways to solve fractional differential equations analytically. One of the most popular and widely used methods is the Laplace transformation. Below, for example, this method is described [13]. Before continuing, it should be noted that in general, the number of initial conditions required for a partial differential equation will depend on the order of the differential equation. However, in a fractional differential equation, the number of the initial condition is equal to the minimum integer order value α [14,15]. Consider the following differential equation.

$$xD_t^{\alpha}y(t) + Ky(t) = f(t) \tag{10}$$

Which y(t) is displacement, k, and τ are constants, as well as the fractional derivative is also Caputo and $0 < \alpha < 1$. In what follows, it has been shown that this partial differential equation model is the dynamics of a purely elastic spring and a viscoelastic element connecting in parallel with a body of mass m, which a force f is applied on a body.[9] To solve, the first step is to take the Laplace transformation of both sides of the original partial differential equation, the Laplace transformation is concisely explained. we have:

$$Y(s) = \frac{f(t)}{x(s^{\alpha} + k/x)}$$
(11)

where α and *s* are fractional order and Laplace domain variable respectively. Also, it is supposed that x(0) = 0. To find the solution, all we need to do is to take the inverse transform:

$$y(t) = \frac{f(t)}{x} t^{(\alpha-1)} E_{\alpha,\alpha}(t) \left(-\frac{k}{x} t^{\alpha}\right)$$
(12)



Which $E_{\alpha,\alpha}$ (t) is Mittag-Leffler function, if the spring is ignored, the equation (10) will be reduced to

$$f(t) = x D_t^{\alpha} y(t) \tag{13}$$

We taking the Laplace transforms of both sides of the equation, simplifying algebraically the result to solve the obtained equation in terms of *s*, and c finally finding the inverse transform, we have:

$$y(t) = Kt^{\alpha} \tag{14}$$

Which $K = f/x\Gamma(\alpha + 1)$. Although the Laplace transformation method is one of the simple and practical methods for solving the fractional equations same as the partial differential equations, most of the fractional equations could not be solved analytically. In what follows, we present a numerical technique to solve Caputo fractional differential equation. So numerical simulations of fractional differential equations need a larger number of floating-point operations and data flow in computer memory systems. This is because, as pointed out by [16], specific additional conditions are needed to solve a differential equation to obtain a unique solution. These additional conditions for the Riemann–Liouville fractional derivative constitute a certain fractional derivative of unknown solution at the initial points which might result in an unclear physical meaning. Due to this reason, in the present work, we consider the fractional Caputo's.

$$y_k^p(t) = y_0(t) + \frac{1}{\Gamma(\alpha)} \sum_{j=0}^{k-1} b_{j,k} f(t_j, y_j),$$
(15)

4. Laplacian Transform Interpretation

Suppose that Y(t) is a quantity whose value in terms of f(t, y) can be achieved as follows:

$$Y(t) = \int_{0}^{t} \frac{(t-x)^{(\alpha-1)}}{\Gamma(\alpha)} f(x) dx$$
 (16)

The output Y(t) can be viewed as a power-weighted sum which stores the previous input of function f(x). Based on the above definition, such system is a non-memoryless system and, in such systems, memory decays at the rate of $y_k^p(t) = t^\alpha - \frac{1}{\Gamma(\alpha)}$.

Applying the Caputo derivative of order α to both sides of the last relation led to

$$D_t^{\alpha}Y(t) = f(t) \tag{17}$$

www.ajrsp.com



As a result, the differential equation governing the system memory Y(t) is described by a fractional derivative [17]. Therefore, the fractional derivative is a good candidate to explain the system with memory. The nature of weighted function determines the type of fractional derivative which describes a system memory. For example, If the weight function of a system is defined by $t^{1-\alpha} / \Gamma(\alpha)$, the Riemann Liouville elements, and by $t^{1-\alpha} \theta(x-t) / \Gamma(\alpha)$ the Caputo elements are used which θ is the Heaviside function [18].

Definition 4.1 Let f(t) be defined for $t \ge 0$. The Laplace transform of f(t), denoted by F(s) or $\mathcal{L}(f(t))$, is an integral transform given by the Laplace integral:

$$F(s) = \mathcal{L}(f(t)) = \int_{0}^{\infty} e^{-st} f(t)dt$$
(18)

Theorem 4.1 The Laplace transform of the Mittage–Leffler function is given by the equation [19]:

$$\mathcal{L}^{-1}\left(\frac{s^{-(\gamma-\alpha)}}{s^{\alpha}-y}\right) = t^{\gamma-1}G_{\alpha,\gamma}(yt^{\alpha}), \quad |s^{\alpha}-y| < 1$$

Proof. Using the definition of the Laplace transform, we have:

$$\mathcal{L}\left(t^{\gamma-1}G_{\alpha,\gamma}(yt^{\alpha})\right) = \int_{0}^{+\infty} e^{-st} t^{\gamma}G_{\alpha,\gamma}(yt^{\alpha})dt = \sum_{i=1}^{+\infty} \frac{y^{i}}{\Gamma(\alpha i + \gamma)} = \int_{0}^{+\infty} e^{-st} t^{\alpha i + \gamma - 1} dt \quad (19)$$

From this equation we get

$$\sum_{i=0}^{+\infty} \frac{y^i}{\Gamma(\alpha i + \gamma)} \mathcal{L}(t^{\alpha i + \gamma - 1}) = \sum_{i=0}^{+\infty} \frac{y^i}{\Gamma(\alpha i + \gamma)} \frac{\Gamma(\alpha i + \gamma)}{S^{\alpha i + \gamma}} = \frac{1}{S^{\gamma}} \sum_{i=0}^{+\infty} \left(\frac{y}{S^{\alpha}}\right)^i$$
(20)

In this series above converges from $\left|\frac{y}{S^{\alpha}}\right| < 1$, hence,

$$\mathcal{L}\left(t^{\gamma-1}G_{\alpha,\gamma}(yt^{\alpha})\right) = \frac{S^{-\gamma}}{1-\frac{y}{S^{\alpha}}} = \left[\frac{S^{-(\gamma-\alpha)}}{S^{\alpha}-y}\right].$$
(21)

4.1. Laplace transform of fractional derivatives for integer order

If f is of integer order, and f is continuous and f_0 is piecewise continuous on all interval [20].



 $0 \le t \le b$: Then:

 $\mathcal{L}(f'(t)) = S\mathcal{L}(f(t)) - f(0)$

Applying the theorem multiple times yields

$$\mathcal{L}(f''(t)) = S^{2}\mathcal{L}(f(t)) - Sf(0) - f'(0)$$

$$\mathcal{L}(f'''(t)) = S^{3}\mathcal{L}(f(t)) - S^{2}f(0) - f'(0) - f''(0)$$

$$\vdots$$

$$\vdots$$

$$\mathcal{L}(f^{(n)}(t)) = S^{n}\mathcal{L}(f(t)) - S^{n-1}f(0) - S^{n-2}f'(0) - S^{n-3}f''(0) - \dots - S^{2}f^{(n-3)}(0)$$

$$-Sf^{(n-2)}(0) - f^{(n-1)}(0)$$
(22)

Significantly, we say that the Laplace transform, when applied to differential equations, will change the derivatives into algebraic expressions in terms of s and the dependent variable t. Thus, the Laplace transform can convert a differential equation into an algebraic equation.

4.2. Laplace Transform of Fractional Differential Operators Definition 4.2 Caputo Fractional Derivative

Assume that the function $f \in \mathbb{C}^n[a, b]$, $\alpha \ge 0$ and $n - 1 < a \le n$. Then we have

$$D^{\alpha}f(t) = \frac{1}{\Gamma(n-\alpha)} \int_{a}^{t} (t-x)^{n-\alpha-1} \frac{\partial^{n}f(x)}{\partial x^{n}} dx, \quad a \le t < b$$
$$= \frac{1}{\Gamma(n-\alpha)} \int_{0}^{t} \frac{f^{n}(x)}{(t-x)^{\alpha+1-n}} dx.$$
(23)

Definition 4.3. The α^{th} order Riemann-Liouville derivative of function is.

$$D^{\alpha}_{\alpha,t}f(t) = \frac{1}{\Gamma(n-\alpha)} \frac{\partial^n}{\partial t^n} \int_{\alpha}^{t} \frac{f(x) \, dx}{(t-x)^{1-\alpha}},\tag{24}$$

and the integral

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54



Publication Date: 05-10-2023 ISSN: 2706-6495

$$I_{\alpha,t}^{\alpha}f(t) = \frac{1}{\Gamma(\alpha)} \int_{\alpha}^{t} \frac{f(x) dx}{(t-x)^{1-\alpha}}$$
(25)

Lemma 4.1. The Laplace transform of Riemann-Liouville fractional integral operator of order $\alpha > 0$ can be obtained in the form:

$$\mathcal{L}(I^n f(t)) = \frac{F(s)}{S^{\alpha}}$$
(26)

Where I^n is the α integral.

Proof. The Laplace transform of Riemann-Liouville fractional integral operator of order $\alpha > 0$ is get:

$$\mathcal{L}(I^{n}f(t)) = \mathcal{L}\left(\frac{1}{\Gamma(\alpha)}\int_{0}^{t}(t-x)^{\alpha-1}f(x)dx\right) = \frac{1}{\Gamma(\alpha)}F(s)G(s)$$

Where is:

$$G(s) = \mathcal{L}(t^{\alpha-1}) = \frac{\Gamma(\alpha)}{S^{\alpha}}$$

And hence

$$\mathcal{L}(I^n f(t)) = \frac{1}{\Gamma(\alpha)} \frac{\Gamma(\alpha)}{S^{\alpha}} F(S) = \frac{F(s)}{S^{\alpha}}$$

Lemma 4.2. The Laplace transform of Caputo fractional derivative for

 $m-1 < \alpha \leq m, m \in \mathbb{N}$, can be obtained in the form of [21, 22]:

$$\mathcal{L}(D_t^{\alpha}f(t)) = \frac{t^m f(t) - t^{m-1} f(0) - t^{m-2} f'(0) - \dots - f^{(m-1)}(0)}{t^{m-\alpha}}$$
(27)

Proof. The Laplace transform of Caputo fractional derivative of order $\alpha > 0$ is:

$$\mathcal{L}(D_t^{\alpha}f(t)) = \mathcal{L}(I^{m-\alpha}f^{(m)}(t)) = \frac{\mathcal{L}(f^{(m)}(t))}{S^{m-\alpha}}$$
(28)

We are ready to see how the Laplace transform can be used in differentiation equations.



4.3. Solving differential equation problems using the method of Laplace transform:

To solve a linear differential equation using Laplace transforms, there are only 3 basics steps:

1. Take the Laplace transforms of both sides of an equation.

2. Simplify algebraically the result to solve for $\mathcal{L}(f(t)) = F(s)$ in terms of *s*.

3. Find the inverse transform of F(s). This inverse transform, f(t), is the solution of the given differential equation. [20,21].

Example 4.1. We Consider the following differential equation:

$$\begin{cases} y'' + 5y' + 6y = 0\\ y(0) = 2, \qquad y'(0) = 1 \end{cases}$$

We transform both sides.

$$\mathcal{L}(y'')(s) + 5\mathcal{L}(y')(s) + 6\mathcal{L}(y)(s) = 0$$

From the equations (22), (28) to find $F(s) = \mathcal{L}(y)$

$$s^{2}\mathcal{L}(y)(s) - 2s - 1 + 5(s\mathcal{L}(y)(s) - 2) + 6\mathcal{L}(y)(s) = 0$$

Find the value

$$\mathcal{L}^{-1}\left(\frac{2s+11}{s^2+5s+6}\right)(t)$$
$$\frac{2s+11}{s^2+5s+6} = \frac{A}{s+3} + \frac{B}{s+2} = \frac{s(A+B) + (2A+3B)}{(s^2+5s+6)}$$

Divide the equation using partial fractions.

$$2s = s(A + B) + 2A + 3B$$

$$\begin{cases}
A + B = 2 \\
2A + 3B = 11
\end{cases}$$

$$2A + 3B - (2A + 2B) = 11 - 2 \times 2 \Longrightarrow B = 7$$

And A = 2 - B = 2 - 7 = -5

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54



Publication Date: 05-10-2023 ISSN: 2706-6495

$$\frac{2s+11}{s^2+5s+6} = \frac{-5}{s+3} + \frac{7}{s+2}$$

$$\mathcal{L}^{-1}\left(\frac{2s+11}{s^2+5s+6}\right)(t) = \mathcal{L}^{-1}\left(\frac{-5}{s+3} + \frac{7}{s+2}\right)(t)$$
$$-5\mathcal{L}^{-1}\left(\frac{1}{s+3}\right) + 7\mathcal{L}^{-1}\left(\frac{1}{s+2}\right)(t) = -5e^{-3t} + 7e^{-2t}$$
$$\mathcal{L}(y'')(s) = s^2\mathcal{L}(y)(s) - sy(0) - y'(0) = s^2\mathcal{L}(y)(s) - 2s - 1$$
$$\mathcal{L}(y')(s) = s\mathcal{L}(y)(s) - y(0) = s\mathcal{L}(y)(s) - 2$$

We apply the Laplace transform to the differential equation.

$$\mathcal{L}(y'')(s) + 5\mathcal{L}(y')(s) + 6\mathcal{L}(y)(s) = 0$$
$$s^{2}\mathcal{L}(y)(s) - 2s - 1 + 5(s\mathcal{L}(y)(s) - 2) + 6\mathcal{L}(y)(s) = 0$$

Then,

$$(s^2 + 5s + 6)\mathcal{L}(y)(s) = 2s + 11$$

So

$$\mathcal{L}(y)(s) = \frac{2s + 11}{s^2 + 5s + 6}$$

Example 4.2. We Consider the following partial differential equation:

$$\begin{cases} \frac{\partial u}{\partial x} = 2\frac{\partial u}{\partial t} + u & x \ge 0, \quad t \ge 0\\ u(x,0) = 6e^{-3x} \end{cases}$$

Given u(x, t) is boundary function for all $x \ge 0$, and $t \ge 0$

We apply the Laplace transform to the partial differential equation.

$$\mathcal{L}\left(\frac{\partial u}{\partial x}\right) = 2\mathcal{L}\left(\frac{\partial u}{\partial t}\right) + \mathcal{L}(u)$$

Assume $\mathcal{L}(u) = V(x, s)$

www.ajrsp.com



Then,

$$\frac{d}{dx}(V(x,s)) = 2[sV(x,s) - u(x,0)] + V(x,s)$$
$$\Rightarrow \frac{d}{dx}(V(x,s)) = 2sV(x,s) - 12e^{-3x} + V(x,s)$$
$$\Rightarrow \frac{d}{dx}(V(x,s)) - (2s+1)V(x,s) = -12e^{-3x}$$

The last equation is an ordinary differential equation.

Example 4.3. We Consider the following differential equation:

$$\begin{cases} y' + 2y = 2te^{-2t} \\ y(0) = -3 \end{cases}$$

We transform both sides.

$$\mathcal{L}(y') + \mathcal{L}(2y) = \mathcal{L}(4e^{-2t})$$
$$s\mathcal{L}(y) - y(0) + 2\mathcal{L}(y) = \frac{2}{(s+2)^2}$$

To find $F(s) = \mathcal{L}(y)$

$$s\mathcal{L}(y) - (-3) + 2\mathcal{L}(y) = \frac{4}{(s+2)^2}$$
$$\mathcal{L}(y)(s+2) + 3 = \frac{4}{(s+2)^4}$$
$$\mathcal{L}(y)(s+2) = \frac{2}{(s+4)^2} - 3$$
$$\mathcal{L}(y) = \frac{4}{(s+2)^3} - \frac{3}{(s+2)} = \frac{4 - 3(s+2)^2}{(s+2)^3} = \frac{-3s^2 - 12s - 8}{(s+2)^3}$$

Divide the equation using partial fractions.

$$\mathcal{L}(y) = \frac{-3s^2 - 12s - 8}{(s+2)^3} = \frac{A}{(s+2)^3} + \frac{B}{(s+2)^2} + \frac{C}{(s+2)} = \frac{A + B(s+2) + C(s+2)^2}{(s+2)^3}$$

www.ajrsp.com



$$\frac{-3s^2 - 12s - 8}{(s+2)^3} = \frac{A + Bs + 2B + Cs^2 + 4Cs + 4C}{(s+2)^3}$$
$$\frac{-3s^2 - 12s - 8}{(s+2)^3} = \frac{Cs^2 + (B + 4C)s + (A + 2B + 4C)}{(s+2)^3}$$

By equating the comparison for both fractions, we obtain:

C = -3, (B + 4C) = -12, (A + 2B + 4C) = -8

Solving the above system, we obtain

$$C = -3, \qquad A = 4, \qquad B = 0$$

Now, by substituting the values in the expression of $\mathcal{L}(y)$, we obtain.

$$\mathcal{L}(y) = \frac{-3s^2 - 12s - 8}{(s+2)^3} = \frac{4}{(s+2)^3} - \frac{3}{(s+2)} \Longrightarrow y(t) = 4\mathcal{L}^{-1}\left(\frac{1}{(s+2)^3}\right) - 3\mathcal{L}^{-1}\left(\frac{1}{(s+2)}\right)$$

And hence

$$y(t) = 4t^2 e^{-2t} - 3e^{-2t}$$

In the next section, we will discuss how to solve differential equation problems for nonlinear fractions order for The Volterra Integral Equation.

5. The Volterra Integral Equation

This method introduced the series which converges to the solution of an initial-value problem. For the initial-value problem with the Riemann-Liouville derivative (24) appropriate sequence can be calculated in the following way. [10,15]:

$$y_0(t) = \sum_{s=1}^n \frac{b_s}{\Gamma(\alpha - S + 1)} (t - a)^{\alpha - S}$$
(29)

$$y_{i}(t) = y_{0}(t) + \frac{1}{\Gamma(\alpha)} \int_{a}^{t} (t - \mu)^{\alpha - S} f(\mu, y_{i}(\mu)) d\mu$$
(30)

Where n is the number of initial conditions, i = 1, 2, 3, ... and $f(\mu, y_i(\mu))$ is the right-hand side of the equation. Hence the solution is:



$$y(t) = \lim_{i \to \infty} y_i(t) \tag{31}$$

This method can be easily applied to nonlinear equations as well. And can Getting a formula in general may be a problem with a specification convergence period. And this method gives the solution in closed form to the linear binomial equation with constant coefficients and even to the equation:

$$D_a^{\alpha} y(t) - \beta(t-a)^{\lambda} y(t) = 0 \Longrightarrow D_a^{\alpha-S} y(a) = b_S$$
(32)

where b_S , β are real constants, S = 1, ..., m and $\lambda > -\alpha$. Because we already know the solution of linear two-term equations with constant coefficients, we will solve the second problem now. Assume that without the proof that the problem (32) satisfies all necessary assumptions to this method [10,22].

Example 5.1. Solve the initial-value problem (29) with the Riemann-Liouville fractional derivative, $n = -[-\alpha]$.

Applying the formulas (30) and (31) we get the expressions.

$$y_0(t) = \sum_{S=1}^n \frac{b_S}{\Gamma(\alpha - S + 1)} (t - a)^{\alpha - S}$$
$$y_i(t) = y_0(t) + \frac{\beta}{\Gamma(\alpha)} \int_a^t (t - \mu)^{\alpha - S} (\mu - a)^{\lambda} y_{i-1}(\mu) d\mu$$

We compute terms $y_1(t)$, $y_2(t)$ and see what happens.

$$y_{1}(t) = y_{0}(t) + \frac{\beta}{\Gamma(\alpha)} \int_{a}^{t} (t-\mu)^{\alpha-S} \sum_{S=1}^{n} \frac{b_{S}}{\Gamma(\alpha-S+1)} (\mu-a)^{\alpha-\lambda-S}$$

$$= y_{0}(t) + \beta \sum_{S=1}^{n} \frac{b_{S}}{\Gamma(\alpha-S+1)} D_{a}^{-\alpha} ((t-a)^{\alpha-\lambda-S})$$

$$y_{0}(t) + \beta \sum_{S=1}^{n} \frac{b_{S}(t-a)^{2\alpha+\lambda-S}\Gamma(\alpha+\lambda-S+1)}{\Gamma(\alpha-S+1)}$$

$$y_{2}(t) = y_{0}(t)\beta D_{a}^{-\alpha} \left((t-a)^{\lambda}y_{1}(t) \right) = y_{1}(t) + \beta^{2} D_{a}^{-\alpha} \left((t-a)^{\lambda} (y_{1}(t) - y_{0}(t)) \right)$$

www.ajrsp.com

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54



Publication Date: 05-10-2023 ISSN: 2706-6495

$$= y_1(t) + \beta \sum_{s=1}^n \frac{b_s(t-a)^{3\alpha+2\lambda-s}\Gamma(\alpha+\lambda-S+1)\Gamma(2\alpha+2\lambda-S+1)}{\Gamma(\alpha-S+1)\Gamma(2\alpha+\lambda-S+1)\Gamma(3\alpha+2\lambda-S+1)}$$

This can be proved in general by our:

$$y_i(t) = \sum_{S=1}^n \frac{b_s(t-a)^{\alpha-s}}{\Gamma(\alpha-S+1)} \left[1 + \sum_{i=1}^j \left(\prod_{\gamma=1}^j A_k \frac{\Gamma(\gamma(\alpha+\lambda)-S+1)}{\Gamma(\gamma(\alpha+\lambda)+\alpha-S+1)} \right) \left(\beta(t-a)^{\alpha+\lambda} \right)^i \right]$$

When we shift the index in the product and consider $m \to \infty$, we obtain the solution of this homogeneous equation containing the generalized function [23,24]:

$$y_n(t) = \sum_{S=1}^n \frac{b_s(t-a)^{\alpha-s}}{\Gamma(\alpha-S+1)} R_{\alpha,1+\frac{\lambda}{\alpha},1+\frac{\lambda-S}{\alpha}} \left(\beta(t-a)^{\alpha+\lambda}\right)$$
(33)

Example 5.2. Solve the equation in the initial-value problem (29) with the Caputo fractional derivative and with initial conditions $y_s(a) = b_s$ for S = 0, ..., n - 1. Here we solve the linear initial-value problem which we discussed generally for sequential derivative before. If we look at the Caputo derivative as its special case, implies the following procedure. Again, by application of (30) and (31) with:

$$y_0(t) = \sum_{s=1}^{n-1} \frac{b_s}{s!} (t-a)^s$$
(34)

By following the same steps above, we obtain the expression for the i^{th} term:

$$y_i(t) = \sum_{s=1}^{n-1} \frac{b_s}{s!} (t-a)^s \left[1 + \sum_{i=1}^j \left(\prod_{\gamma=1}^j A_k \frac{\Gamma(\gamma(\alpha+\lambda) - S + 1)}{\Gamma(\gamma(\alpha+\lambda) + \alpha - S + 1)} \right) \left(\beta(t-a)^{\alpha+\lambda} \right)^i \right]$$
(35)

Then we are using a limit and shift of the index we get the solution:

$$y_i(t) = \sum_{s=1}^{n-1} \frac{b_s}{s!} (t-a)^s R_{\alpha,1+\frac{\lambda}{\alpha'}\frac{\lambda+s}{\alpha}} (\beta(t-\alpha)^{\alpha+\lambda})$$
(36)

We derived the solution of the homogeneous equation (34) with appropriate initial conditions in the Riemann-Liouville and the Caputo senses. It can be proven that the functions in the sums which form both solutions, are independent [5]. We saw that due to the linearity it is



not difficult to obtain the formula for the i^{th} term of the series and then to pass to the limit. Generally, the situation is not so simple.

$$\lim_{i \to n} \sum_{i=1}^{n-1} \frac{b_i}{i!} \ (t-a)^i$$

6. The Caputo Fractional Differential

Definition 6.1 (Caputo Fractional Derivative)

Assume the function $f \in \mathbb{C}^n[a, b]$, a > 0 and $n - 1 < \alpha \le n$, then,

$$D_t^{\alpha} f(t) = \frac{1}{\Gamma(n-\alpha)} \int_a^t (t-x)^{n-\alpha-1} \frac{\partial^n f(x)}{\partial x^n} dx = \frac{1}{\Gamma(n-\alpha)} \int_a^t \frac{f^{(n)}(x)}{(t-x)^{\alpha+1-n}} dx, \quad a \le t$$
$$\le b, \quad (37)$$

The benefit of using the Caputo definition is that it does not only allow for the consideration of easily interpreted initial conditions, but it is also bounded, meaning that the derivative of a constant is equal to 0 [11,24].

Theorem 6.1. Fundamental Theorem of Calculus (FTC)

Let f(x) be a continuous real-valued function defined on a closed interval [a, b] and Let f be a real-valued function on a closed interval [a, b] and F an antiderivative of f in [a, b].

$$F(x) = \int_{a}^{x} f(x) dx, \qquad \forall x \in [a, b].$$
(38)

Then, F(x) is uniformly continuous on [a, b] differentiable on the open interval (a, b), and

$$F'(x) = f(x), \qquad \forall x \in (a, b)$$
(39)

If f is Riemann integrable on, [a, b] then.

$$\int_{a}^{b} f(x) \, dx = F(b) - F(a) \tag{40}$$



f(x) is n^{th} differentiable on [a, b] then it is continuous since $f \in Cn[a, b]$ and $(t - x)_{n-\alpha-1}$ is continuous on the interval [0, t) Since

 $f^{(n)}(x)$ is bounded on [a, b], and $-1 < n - \alpha - 1 \le 0$, then

$$\frac{f^{(n)}(x)}{(t-x)^{\alpha+1-n}}$$

Is integrable over [0, t], where $a \le t \le b$. Thus, by FTC, $\frac{f^{(n)}(x)}{(t-x)^{\alpha+1-n}}$ is differentiable and then it is continuous [5,25].

Example 6.1 Find the second derivative of $f(x) = x^3$ using Caputo definition. From equation (37), we have.

$$D_t^{\alpha} f(t) = \frac{1}{\Gamma(n-\alpha)} \int_0^t (t-x)^{n-\alpha-1} \frac{\partial^n f(x)}{\partial x^n} dx, \qquad 0 \le t < b$$

If n = 3, $\alpha = 2$ then,

$$D_t^2 f(t) = \frac{1}{\Gamma(3-2)} \int_0^t (t-x)^{3-2-1} \frac{\partial^3 f(x)}{\partial x^3} dx,$$

For $f(x) = x^3 \implies f'(x) = 3x^2$, f''(x) = 6x, and f'''(x) = 6

Then,

$$D_t^2 f(t) = \frac{1}{\Gamma(1)} \int_0^t (t-x)^0 \ 6 \ dx = \int_0^t 6 \ dx = 6t$$

Note that $\Gamma(1) = 1$

Example 6.2. Find the half derivative of $f(x) = x^3$ using Caputo definition. so n = 3 and $\alpha = 1/2$,

$$D_t^{\frac{1}{2}}f(t) = \frac{1}{\Gamma\left(3-\frac{1}{2}\right)} \int_0^t (t-x)^{3-\frac{1}{2}-1} \frac{d^3 f(x)}{dx^3} dx,$$



Using the previous example, we have f'''(x) = 6 then, we have,

$$D_t^{\frac{1}{2}} f(t) = \frac{1}{\Gamma\left(\frac{5}{2}\right)} \int_0^t (t-x)^{\frac{3}{2}} 6 \, dx = D_t^{\frac{1}{2}} f(t) = \frac{6}{\Gamma\left(\frac{5}{2}\right)} \int_0^t (t-x)^{\frac{3}{2}} \, dx$$

Using the properties of Gamma function, the integral becomes formula,

$$D_t^{\frac{1}{2}} f(t) = \frac{6 \cdot 2}{5 \cdot \Gamma\left(2 + \frac{1}{2}\right)} \left(t - x\right)^{\frac{3}{2} + 1} \Big|_0^t = \frac{12}{5 \cdot \frac{3}{4}\Gamma\left(\frac{1}{2}\right)} \left(-t\right)^{\frac{5}{2}} = \frac{8}{15\sqrt{\pi}} \cdot \left(-t\right)^{\frac{5}{2}}$$



Figures 6.1 (1)-(2)

Remark 6.1. The fractional derivatives and integrals of function $f(x) = x^3$ in example 6.1 and 6.2 plotted in Figures 6.1 (1)-(2) are computed by applying definition 6.1 and Theorem 6.1. The fraction derivatives and integrals of $f(t) = t^3$ are evaluated by the application of Lemma 4.2. The fractional derivatives and integrals of trigonometric and hyperbolic functions can be evaluated using the relation between Volterra Integral function and generalized trigonometric functions (35), generalized hyperbolic functions (37). But the numerical evaluation of the Volterra Integral functions is itself difficult. We have used a much simpler method based on the Haar wavelets, to evaluate the fractional integrals of some functions of Caputo Fractional Differential. For the classical cases. $\alpha = 2$, $\frac{1}{2}$. The obtained results by the Haar wavelets are in



good agreement with the exact values. For $f(t) = t^3$ and $\alpha = 2, \frac{1}{2}$, the maximum absolute error is $6.5 \times 10^{-4} \times 10^{-4}$ and $\frac{8}{15\sqrt{\pi}} \times 10^{-5}$ respectively.

7. Conclusions

The classical tools from functional analysis operator theory, on existence to boundary value problems for nonlinear fractional differential equations, with the. Laplacian Transform Interpretation and the Caputo fractional derivatives, Volterra Integral Equation, Caputo Fractional Differential is developed, we established sufficient conditions for existence results for different classes of nonlinear boundary value problems involving fractional derivatives, subject to integral boundary conditions. Several existence results for positive and multiple positive solutions to different ways of boundary value problems for fractional differential equations are obtained. For the value problem (1), the existence of at least one positive solution is guaranteed in a specially constructed cone in the Laplace transform of Riemann-Liouville fractional integral operator. It is observed that functions (22) and (23) for the value problem (28), satisfy some interesting the Volterra Integral Equation, Caputo Fractional Differential and useful properties and they are related to each other. This helps us to construct a cone in the partial differential equation model. Then we established existence results for positive solutions in this cone.

8. References

- Furati, K.M. and M.D. Kassim, *Existence and uniqueness for a problem involving Hilfer fractional derivative*. Computers & Mathematics with applications, 2012. **64**(6): p. 1616-1626.
- 2. Hilfer, R., Applications of fractional calculus in physics. 2000: World scientific.
- Oldham, K.B., *Fractional differential equations in electrochemistry*. Advances in Engineering software, 2010. 41(1): p. 9-12.
- Magin, R.L., *Fractional calculus models of complex dynamics in biological tissues*. Computers & Mathematics with Applications, 2010. **59**(5): p. 1586-1593.
- Veeresha, P., D. Prakasha, and H.M. Baskonus, New numerical surfaces to the mathematical model of cancer chemotherapy effect in Caputo fractional derivatives. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2019. 29(1).



- 6. Kilbas, A.A., H.M. Srivastava, and J.J. Trujillo, *Theory and applications of fractional differential equations*. Vol. 204. 2006: elsevier.
- 7. VEIT, J., Integrals' transform ace. Praha: SNTL, 1983. 120 p.
- Schumer, R., et al., *Eulerian derivation of the fractional advection–dispersion equation*. Journal of contaminant hydrology, 2001. 48(1-2): p. 69-88.
- Benson, D.A., *The fractional advection-dispersion equation: Development and application*.
 1998: University of Nevada, Reno.
- Benson, D.A., S.W. Wheatcraft, and M.M. Meerschaert, *The fractional-order governing* equation of Lévy motion. Water resources research, 2000. 36(6): p. 1413-1423.
- BAYIN, S., *Mathematical Methods in Science and Engineering*. 679 p, ed. I. 978-0-470-04142-0. Vol. ISBN 978-0-470-04142-0. 1983, United States: JohnWiley & Sons, Inc. 679 p.
- 12. Abdulaziz, O., I. Hashim, and S. Momani, *Solving systems of fractional differential equations by homotopy-perturbation method.* Physics Letters A, 2008. **372**(4): p. 451-459.
- 13. Podlubny, I., *Fractional differential equations: an introduction to fractional derivatives, fractional differential equations, to methods of their solution and some of their applications.* 1998: Elsevier.
- 14. Diethelm, K., *Efficient solution of multi-term fractional differential equations using P (EC) m E methods*. Computing, 2003. **71**: p. 305-319.
- Diethelm, K., N.J. Ford, and A.D. Freed, *Detailed error analysis for a fractional Adams method*. Numerical algorithms, 2004. 36: p. 31-52.
- Agarwal, R.P., V. Lakshmikantham, and J.J. Nieto, On the concept of solution for fractional differential equations with uncertainty. Nonlinear Analysis: Theory, Methods & Applications, 2010. 72(6): p. 2859-2862.
- Agarwal, R.P., M. Benchohra, and S. Hamani, A survey on existence results for boundary value problems of nonlinear fractional differential equations and inclusions. Acta Applicandae Mathematicae, 2010. 109: p. 973-1033.
- 18. Herrmann, R., Fractional calculus: an introduction for physicists. 2011: World Scientific.
- Ahmad, B. and S. Sivasundaram, On four-point nonlocal boundary value problems of nonlinear integro-differential equations of fractional order. Applied Mathematics and Computation, 2010. 217(2): p. 480-487.


- Ahmad, B. and J.J. Nieto, *Existence results for a coupled system of nonlinear fractional differential equations with three-point boundary conditions*. Computers & Mathematics with Applications, 2009. 58(9): p. 1838-1843.
- Al-Mdallal, Q.M., M.I. Syam, and M. Anwar, *A collocation-shooting method for solving fractional boundary value problems*. Communications in Nonlinear Science and Numerical Simulation, 2010. 15(12): p. 3814-3822.
- 22. Kumar, P. and O.P. Agrawal, *An approximate method for numerical solution of fractional differential equations*. Signal processing, 2006. **86**(10): p. 2602-2610.
- 23. Li, Z.-B., *An extended fractional complex transform*. International Journal of Nonlinear Sciences and Numerical Simulation, 2010. **11**(Supplement): p. 335-338.
- Zhang, S., L. Hu, and S. Sun, *The uniqueness of solution for initial value problems for fractional differential equation involving the Caputo-Fabrizio derivative*. Journal of Nonlinear Sciences & Applications (JNSA), 2018. 11(3).
- Atangana, A. and J. Gómez-Aguilar, Numerical approximation of Riemann-Liouville definition of fractional derivative: from Riemann-Liouville to Atangana-Baleanu. Numerical Methods for Partial Differential Equations, 2018. 34(5): p. 1502-1523.

Copyright © 2023 Dr. Mariam ALmahdi Mohammed Mulla. This is an Open-Access Article Distributed under the Terms of the Creative Commons Attribution License (CC BY NC) **Doi:** <u>https://doi.org/10.52132/Ajrsp.e.2023.54.4</u>



Psychological Stress and its Relationship to Achievement Motivation among Middle School Teachers in Palestinian Schools in Qatar in Light of Corona Crisis

Dr. Dunia Rajeh Moqpil

PhD researcher, Department of Human Sciences, University of Sfax, Tunisia Email: <u>muqbeld7@gmail.com</u>

Dr. Mohammed jarraye

Professor, Department of Human Sciences, Higher Institute of Sport and Physical Education of Sfax, University of Sfax, Tunisia

Email: mohamed.jarraya@isseps.usf.tn

Abstract:

This study aims to identify the relationship between psychological stress and achievement among male and female teachers in Palestinian schools in light of the Corona Virus (COVID-19) crisis in the State of Qatar. The researcher used the descriptive survey method. The current study population consisted of 56 Palestinian school teachers in the State of Qatar chosen intentionally and the exploratory study was conducted on a sample consisting of (10) teachers. To answer the research questions, the researcher followed some statistical methods; Pearson Correlation Coefficient to verify the stability of the measures by applying and re-application, Cronbach Alpha correlation coefficient to verify the stability of the scales by calculating internal consistency. In the first question, the researcher found that all items of the psychological pressures scale came with a high degree as the mean was (2.46) with standard deviation (0.05)which can be explained that most teachers work under psychological stress especially after COVID crise. The answer to the second question related to the level of motivation, the results came to show that most items had a moderate level with mean (3.67) with standard deviation (0.44). Based on the results, the researcher recommended firstly adopting methods that enhance achievement motivation and reduce the extent of psychological pressure among male and female teachers.

Keywords: Anxiety, achievement, teachers, the Corona crisis



1. Introduction

The phenomenon of psychological stress is one of modern times and one of the psychological phenomena affecting the mental health of the individual. The severity of psychological stress and repeated exposure may result in adverse effects on the individual's personality and a mental health imbalance that may affect the individual's health. Hence, the word "pressure" has become one of the common and familiar words of our present time, as the individual is subjected to the pressure of life and daily work, which significantly affects him internally and externally and in his dealings with others as well as his daily behaviour (Mr. Abdelmonim, 2001:5).

Pressure occurs in the absence of a real or substantive balance between the individual's perceived demands and his ability to respond to these perceived demands as Hans Seley - one of the pioneers in psychological pressures- has defined the notion of pressure as a body-neutral response to any requirement (Mohamed Alawi, 1998:402). Recent studies in the field of psychology have demonstrated the great interest in the phenomenon of psychological stress to which individuals are subjected because of its severe impact on their daily performance, as well as its impact on various aspects of the personality, including the motivational aspects that result in exhaustion and stress and the player cannot resist it.

Motivation for achievement is an important aspect of the system of human motivation and has emerged as one of the hallmarks of study and research into the dynamics of personality and behaviour, and can even be regarded as one of the achievements of contemporary human thought (El Safi, 2001). The use of the term "motivation for achievement in psychology" is historically attributable to Adler, who noted that the need for achievement was a compensatory motive derived from childhood experiences. Levin, who introduced the term in the light of his approach to the concept of ambition, and despite these early beginnings, it was credited to the American scientist Murray who was the first to introduce the concept of the need to deliver accurately (Engler, 1991).

The accomplished individual has the privilege of making an effort and continuing to try for success. He also tends to solve problems and persevere in solving them even if he is not under external pressure to do so and always strive to reach the advanced positions in work and society (Moses, 2003).



Coronaviruses are a broad clique of viruses that include viruses that can cause a range of disorders in humans, ranging from the normal cold to severe acute respiratory syndrome. Viruses from this clique also cause a number of animal diseases; this particular strain of coronavirus has never been identified in human. Information on COVID 19 transmission, infections and clinical impact is very limited as the number of reported cases has so far been small.

Hence, the researcher recognized the importance of research on this topic, which links very important factors in educational psychology researches in order to get closer to the stage of implementing and production. To serve her community, the researcher noted the lack of studies on the subject of psychological stress and achievement, especially in the light of COVID 19 crisis in the field of education in the Arab homeland.

1.1. The problem and importance of the study:

Psychological stress is an important phenomenon in the field of education because of its severe impact on the individual therefore it was addressed by many researchers to clarify its relationship to some psychological variables. The problem of research can be seen in the fact that psychological pressures have a clear impact on the personality and some personal variables such as anxiety, aggression and motivation to accomplish, where people's performance is influenced whether by the severity of psychological pressures or its lackness (Izzat Mahmoud Al-Kashif, 1991:4).

The interest in studying achievement motivation is due to its importance in many applied and practical fields, including the educational field and the academic field. Motivation for achievement is an important factor in directing and activating an individual's behavior, in perceiving situations, and in understanding and interpreting the individual's behavior and the behavior of those around him. Motivation for achievement is also expressed as a crucial element in the individual's struggle towards self-realization and self-affirmation, as the individual feels self-fulfillment depending on what he achieves, what goals he achieves, what is the best way of life that he seeks, and higher levels of human existence he searches for. The need for achievement can be one of the strongest influences on motivation and interest in one's life. (Abdul Latif Khalifa, 1997)

The world recently witnessed a great event that threatened education with a huge crisis that was perhaps the most dangerous in our contemporary era.

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54 Publication Date: 05-10-2023 ISSN: 2706-6495



The Coronavirus (COVID-19) pandemic has caused more than 1.6 billion children and youth to be out of school in 161 countries, nearly 80% of the students enrolled in schools around the world. This came at a time when we are already experiencing a global educational crisis. There were many students in the schools, but they did not receive the basic skills they needed in working life. The World Bank's index of "learning poverty" - or the proportion of students who cannot read or understand by the age of 10 - shows that before the outbreak, the proportion of such children in low- and middle-income countries was 53. %. If we do not act, this pandemic may make that outcome worse. (36)

During the world's confrontation with Corona, the researcher worked in the field of education in Palestinian schools in Qatar. She noticed that psychological disorders are prevalent among male and female teachers in schools, which affects their performance and level of achievement. The researcher suggested that psychological disorders are the psychological factor that affects the level of achievement at work and thus achieving the desired goal of the educational process. Therefore, the researcher decided to conduct this study, which would determine the level of psychological disorders and the level of achievement in light of the Corona pandemic.

1. What is the level of psychological stress among male and female middle school teachers in Palestinian schools in Qatar in light of the Corona crisis in Palestinian schools in Qatar?

2. What is the level of achievement motivation for male and female middle school teachers in Palestinian schools in Qatar in light of the Corona crisis in Palestinian schools in Qatar?

3. Is there a relationship between psychological pressures and motivation for achievement among male and female middle school teachers in Palestinian schools in Qatar in light of the Corona crisis in Palestinian schools in Qatar?

1.2. Research Terms:

Psychological stress

Muhammad Allawi (1998) defines the stress in the sports field as the pressures associated with the intertwined and complex relationships between the player and the coach, the administrator, the fans, the media and others who have many relationships with the players in the sports environment and what may be associated with the quality of these relationships in terms of criticism or lack of sufficient appreciation, a lack of motivation, encouragement or an attempt to demand the achievement of an exaggerated level of ambition (39).



Achievement motivation

Al-Widyan (2000: 74) defined it as "the feeling of comfort and satisfaction when accomplishing something or finding something that did not exist."

Coronavirus disease (COVID-19)

Known as acute respiratory illness associated with the 2019 novel coronavirus, it is a zoonotic infectious respiratory disease caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) * (37)

1.3. Study limitations

- Human limit: This study was applied to (52) male and female teachers from Palestinian schools in Qatar.
- Time limit: This study was applied in the academic year 2001/2022.
- Place limit: The study was conducted in Palestinian schools in Qatar.
- Objective limit: Generalizing the results of this study is determined by the validity and reliability of the study tools, and the response of male and female teachers to the questionnaire items.

2. Theoretical framework

First, psychological stress:

Psychological stress are considered one of the psychological phenomena that affect the psychological health of the individual. The intensity of psychological pressures and repeated exposure to it may lead to negative effects and influences on the individual's personality and to a defect in psychological health, which may affect his health and may lead to psychological exhaustion, muscular and mental fatigue, and some problems as negative psychological states that the individual cannot ignore or adapt to easily. Therefore, they are stressful situations that are capable of triggering severe behavioral disorders, and may last for a long time. These situations vary depending on the psychic structure of the individual.

Stressful situations may lead to negative physiological changes, including decreased health efficiency, increased fatigue with minimal effort, difficulty breathing, back pain, and muscle spasm. Likewise, a stressful situation may lead to emotional manifestations, including unpleasant



feelings, and the early stages of depression including anxiety, anger, and lack of emotional control, aggression and jealousy.

Life's psychological pressures impose on the individual requirements that may be physiological, psychological, or social, and may combine two or more of these aspects. Addressing and confronting these pressures results in many damages that the individual bears and affects his personal and professional life (Al-Sayyed Mustafa 2001: 10, 11).

Physical education is considered one of the exhausting professions that are exposed to psychological pressure due to the manifestations of civilizational progress in the modern era in which we live, especially since physical education is a continuous dynamic process whose goal is not only the acquisition of knowledge and meanings and the physical and motor improvement, but in addition to that it works to develop the individual to be a good and useful citizen to his community. (Sabri Imran 1996: 10, 11).

Second, stress:

Stress is known in many meanings and may be defined, for example, as an environmental variable, such as increased public pressure, while others define it as an emotional response to a specific emotional situation such as a young athlete who suffers from high levels of pressure after failure (Osama Al-Asfar 1999: 13).

Samira Muhammad, citing Hans Selye, points out that many environmental factors changes the supposed state of balance of the human body, which leads to the body making different reactions to restore balance. These actions have been called psychological stress or stress triggers that includes anything that requires the body to mobilize its responses. The body responds to stress with an organized system of physical and chemical variables that help the individual to confront or escape from it (Jamal Al-Sayyed 2001: 20).

Barontal et al. (1995) also presented a definition of psychological stress as an interactive element that contains three components: environmental needs, the individual's capabilities, and weak costs between them, which cause poor adaptation between the individual and his surrounding environment.

William Al-Khouli also defined stress as the cases in which a person is exposed to material, moral, environmental, physical and psychological difficulties that he tries to overcome in his daily life in one way or another by adapting to the surrounding environment in an attempt to



maintain a state of balance or compatibility and stability. These difficulties include fatigue, stress, and exhaustion, which are difficult to overcome to restore this balance and stability (Mohamed El-Sheshtawy 2000: 11).

Some researchers have also defined stress in light of three important aspects, the first of which is the stimuli, which are the causes that lead to stress, the second is the response, that is, the individual's current state of stressful situations, and the third aspect examines stress in light of the stimuli and the response together as another aspect.

Third, achievement motivation

Psychology seeks to study human behavior, to find the relationship between behavior and the factors - internal and external - that cause this behavior, and to identify the reason that drives the student to this behavior. Scientists have developed two assumptions to study behavior: behavior is caused, and behavior is intentional (Abu Rayash, Al-Safi, Amour, and Sharif, 2006).

Abu Jadua (2011: 292) defines motivation as "the internal or external states that move the student's behavior and direct him towards achieving a specific goal or purpose, and maintain its continuity until the goal is achieved."

Achievement motivation is defined as "a multi-dimensional hypothetical construct that directs and motivates the individual to carry out his duties accurately, orderly, and independently, and to work to overcome the obstacles he encounters, which instills confidence and reassurance in himself, with the aim of achieving standards of excellence, and achieving near and distant future goals" (Attia, 2002: 31).

Murray also defined it as "focusing on achieving things that others find difficult, controlling the environment and thoughts as well as speed of performance, overcoming obstacles, achieving standards of excellence, discussing with others, and excelling over them" (Al-Fahal, 2000: 7)

Among the theories that have emerged in explaining achievement motivation is Atkinson's theory, which links an individual's expectation of his performance, his self-awareness of his ability, and the consequences thereof, and considers them mutual cognitive relationships that stand behind achievement behavior. Individuals with high achievement motivation make great efforts in attempts to reach a solution to problems (Atkinson, 1960).



The theory emphasizes that the tendency or inclination to achieve success is something acquired, it can be learned, and it varies between individuals, and differs from one individual in different situations. This motivation is affected by three main factors: the motivation to achieve success, the probability of success associated with the difficulty of the task, and the driving value of success (Petri and Govern, 2004). High achievement motivation also increases the ability of individuals to control them in working diligently to solve the problem, and it enables them to develop solid plans to follow them diligently to reach the solution (Ball, 1977).

Individuals with high motivation for achievement are distinguished by their ability to develop reasonable and logical future visions in their perceptions of the problems they face, which are characterized by being moderately difficult and achievable (Bohamama, Abdel Rahim, and Al-Shahoumi, 2006).

High-level achievement motivation motivates its individuals to face problems, confront them, try to solve them, and overcome all the difficulties and obstacles they encounter. Individuals with high achievement motivation are happy when performing moderately difficult tasks and they strive with great enthusiasm towards work. In the contrast, individuals with low achievement motivation avoid problems and quickly stop solving them when they encounter difficulties. This contributes to maintaining high levels of student performance without external monitoring. This is evidence to the positive relationship between achievement motivation, perseverance in work, and good performance, regardless of the mental abilities of learners. Thus, achievement motivation - as currently measured - is a good way to predict academic behavior related to success or failure in the future (Alawneh, 2004).

Individuals who have a high motivation to achieve can work harder than others, and achieve more successes in their lives and in many life situations. When these individuals are compared to those with the same level of mental ability but have a low motivation to achieve, it is found that the first group scores better marks in the speed test to complete arithmetic and verbal tasks, and in solving problems, and they obtain better school and university grades. They also achieve clearer progress in society, and those with high achievement motivation are realistic in seizing opportunities, unlike those with low achievement motivation who accept a simple reality, or aspire to a greater reality much more than their ability to achieve (Santrrock, 2003).



There are differences between those with low and high achievement motivation. Research results in this field have shown that those with high motivation are more successful in school, get promotions in their jobs, and have more success in managing their businesses than those with low motivation. Likewise, those with high motivation tend to choose medium-difficult tasks that contain more than a challenge, and they avoid very easy tasks because there is no challenge in them. Moreover, because of the high probability of failure in them, they also avoid very difficult tasks. Another distinctive characteristic of people with high motivation is that they have a strong desire to obtain feedback about their performance. Therefore, they prefer tasks and jobs in which rewards are based on individual achievement, and do not desire tasks in which rewards are equal (Alawneh, 2004).

Sources of achievement motivation

Students' achievement motivation is attributed to internal and external reasons;

First: Internal sources:

It is one in which the student attributes his achievements to his effort and perseverance in doing the work that achieves the goals. He willingly accepts work and continues to motivate him as long as he achieves success and enjoys its results (Rateb, 1990).

Second: External sources:

The student attributes his success or failure to external factors beyond his control.

There are other classifications of sources of achievement motivation, including (Bani Younis, 2001):

1. Behavioral sources: These are responses to innate causes or stimuli. He performs the action that is followed by reinforcement and avoids the behavior that is followed by a feeling of discomfort or after which he is subjected to punishment.

2. Social sources: where the student imitates socially acceptable behaviors according to community standards.

3. Cognitive resources: They carry out behavior to reach understanding, reach a state of cognitive balance, solve problems, and make appropriate decisions.

4. Emotional sources: These are related to the individual's ability to feel better by reducing threats to his self-concept.



5. Dispositive sources: It depends on facing challenges, reaching the goal, and reaching the level of self-efficacy, through methods that help him control all aspects of life.

6. Spiritual sources: They result from the individual's knowledge of the meaning of his existence, which is the connection between man and his Lord, and performing work that pleases God Almighty.

There are some reasons that reduce students' achievement motivation, including: the nature of a person's achievement motivation, the environment surrounding the person in terms of physical and social aspects, the person's experiences of success and failure, and his expectations about performance (Rashwan and Ali, 2006).

3. Previous studies:

First: Studies that dealt with stress

Gamal Al-Sayed (2001) conducted a study to identify the psychological stress associated with sports competition among young athletes, where the researcher used the descriptive approach, and the research sample included (300) young athletes, then they were randomly selected with an average age of 14-18 years. The researcher used a measure of stress and psychological burnout. The results of the study reached the following: -

- There are statistically significant differences in the psychological pressures associated with competition according to the type of sporting activity chosen.

- There are statistically significant differences between junior players and first-class players in favor of junior players in the psychological pressures associated with competition.

Sabry Omran (2001) aimed to identify the psychological pressures of athletes in the Arab Republic of Egypt, where the researcher used the descriptive approach, the survey method, on a sample of (728) athletes, including (360) male and female team sports players, and (368) individual sports players. The researcher prepared a psychological stress scale as a tool to identify stress. The results of the research led to the construction of a scale for psychological stress.

It includes ten dimensions stress (the public - personal problems - media - rewards and incentives - the relationship with the coach - control and capabilities - injury - management - the relationship and colleagues).



In addition, whether in individual or team games, players are exposed to different stress according to the nature of the activity. First-level players are affected by psychological pressures more than second-level players due to individual or group activities, male or female players.

Osama Al-Asghar (1999) study aimed to identify the sources of psychological stress among young athletes. To fulfill his aim, the researcher used the descriptive method whereas he pointed a sample of (430) players from various activities, and the results of the analysis showed that the most important sources of psychological stress

Among young athletes are: -

- Psychological stress related to training duties and loads.
- Psychological stress related to sports competition (before during after) the competition.
- Psychological stress related to family attitudes towards sports.
- Psychological stress related to the technical and administrative staff, the public, and team members.
- Psychological stress related to the requirements of young people (study time management).

The study concluded that the sources of stress increase for the benefit of team-game players.

Weinberg and Gould (1995) study identified the most important sources of psychological stress facing high-levels athletes. It was conducted on a sample of (300) players from various sports. The results showed that the most important sources of stress facing high-level athletes are:

- Increased training and competition pressures.
- Not enjoying training or competition.
- Setting goals that are more ambitious than the athlete's capabilities.
- Negative response to training stress.
- Increased feeling of excessive fear.
- The lack of appropriate rest periods allows the athlete to recover and gather strength.

Tarry, Gary, and Kenneth (1991) study aimed to identify the sources and causes of psychological stress experienced by high-level athletes in the sport of snowboarding.



The descriptive approach was used on the sample of (26) players. The following tools were used (personal interview - checklist to identify sources of pressure). The most important results indicated a group of sources of pressure facing elite athletes (the highest), arranged as follows:

- Excessive training pressures.
- The pressures of sports competition.
- Negative relationship with others.
- Personal characteristics of athletes.
- Failure experiences.

Second: Studies that dealt with achievement motivation

Al-Safi's study (2000) aimed to identify the relationship between the type of attribution of academic success and failure and achievement motivation. The study sample consisted of 100 students who excelled academically and 100students who fell behind academically. The sample was chosen from the students of the College of Education and the College of Arabic Language at King Khalid bin Abdul Aziz University. The researcher used the attribution scale and the achievement motivation test. The results showed that the outstanding students attributed their success to their effort, ability, study materials, test, teacher's mood, and most recently luck. On the other hand, students who were behind in university attributed their failure to reasons like the teacher, mood, luck, ability, academic materials, test, and finally effort. The results also showed that outstanding students with high achievement motivation attributed their success to ability, effort, study materials, and the test, while academically lagging students with low achievement motivation attributed their failure to mood, luck, and the teacher.

Gok & Silay's study (2009) aimed to determine the effect of applying a problem-solving strategy in education on students' achievement in physics, their attitudes toward solving problems, and achievement motivation, the study sample consisted of (46) male and female students from a secondary school in Turkey. It was divided into an experimental group (12 female students and 13 male students) who were taught using the problem-solving strategy, and a control group (8 female students and 13 male students) who were taught in the usual way. The researcher used an achievement test in physics, a questionnaire about the attitude toward solving problems, and a questionnaire to determine the extent to which students employ themselves in solving problems and the achievement motivation questionnaire.



The results showed the effectiveness of the problem-solving strategy in achievement, motivation and attitudes, and there were no statistically significant differences in achievement attributable to gender.

Al-Ghamdi's study (2009) aimed to find out the differences between academically excellent students and average students in thinking, self-concept, and achievement motivation, the study sample consisted of (400) high school students in the cities of Mecca and Jeddah. The researcher used a scale of rational and irrational thoughts, the self-concept measure, and the achievement motivation measure to achieve the goals of the study. The results showed the spread of rational thinking among outstanding students and the spread of irrational thinking among ordinary students. There is a correlation between rational thinking and self-concept among the outstanding students and among the total sample, while there is no relationship among the ordinary students. There is also a correlation between rational thinking and achievement motivation among the total sample, while there is no relationship among the ordinary. There is also a correlation between rational thinking and achievement motivation among the total sample, while there is no relationship among the ordinary. There is also a correlation between rational thinking and achievement motivation among the total sample, while there is no relationship among the ordinary. There is also a correlation between rational thinking and achievement motivation among the total sample, while there is no relationship among the ordinary. There is also a correlation between self-concept and achievement motivation among ordinary people and the total sample while there is no relationship among ordinary people and the total sample while there is no relationship among ordinary people and the total sample while there is no relationship among ordinary people and the total sample while there is no relationship among ordinary people.

Al-Qabali (2009) aimed to determine the effectiveness of an enrichment program based on smart games in developing problem-solving skills and motivation for achievement among outstanding students in the Kingdom of Saudi Arabia. The study population consisted of 32 students from the third intermediate grade in the Kingdom's schools, distributed into two groups: the first experimental group, consisting of 16 students, and the second group, control, consisting of 16 students. Two tools were used to collect data: the first tool, a measure of problem-solving skills, and the second tool, a measure of achievement motivation. To achieve the goal of the study, an enrichment program was built based on cognitive theory consisting of 20 training sessions, and was applied to members of the experimental sample during the second semester of the year 2008/2009, and the results of the study showed that there were statistically significant differences between the average scores of the experimental and control groups on the problem-solving skills scale, attributed to the enrichment program and in favor of the experimental group.



Shaheen (2012) aimed to identify the effect of successive formative tests in general science for the ninth grade on academic achievement, achievement motivation, and reflective practices. To achieve the goal of the study, the researcher used the experimental method on two samples: the first was 56 male students from the ninth grade in the city of Hebron, who were divided into two experimental and control groups. The second sample was 89 female students, who were divided into two experimental and control groups. The researcher used four formative tests and a final achievement test in addition to the questionnaire. The results of the study showed statistically significant differences between the averages of student achievement according to the two group variables, in favor of the experimental groups, and gender, and in favor of females, while no significant effect was found for the interaction of group and gender. It also became clear that there were no statistically significant differences between the levels of achievement motivation according to the variables of the study, while it was found that there were statistically significant differences were found according to the variables of group and the interaction between group and gender.

Comment on previous studies:

This study agreed in terms of the place of application of the study and the age group of the sample members with the study of Al-Safi (2000), and with the study of (Al-Ghamdi, 2009) and (Al-Qabali, 2009) in terms of place only with the difference in the age group of the sample members.

All the studies that dealt with the issue of psychological stress agreed with this study in terms of using the descriptive approach. As for the studies that dealt with achievement motivation, some of them used the semi-experimental approach, such as the study of (Gok & Silay, 2009) and (Al-Qabbali, 2009; Shaheen, 2012).) which dealt with achievement motivation as a dependent variable, and most of the descriptive studies that were dealt with, especially in the field of psychological stress, used the questionnaire as a tool for data collection. As for the studies that dealt with achievement motivation, measures of achievement motivation were used as in this study.

This study was distinguished from previous studies in that it dealt with psychological pressures at all stages, which the researcher, to her knowledge, did not find any study that addressed it from male and female teachers.



4. Study method and procedures

This part deals with describing the methodology of the current study, the study population and sample, how to build the study tools, the procedures that were followed in the study, and the statistical treatments that were relied upon in analyzing the data.

4.1. Study Methodology: The descriptive approach was used in this study because it suits its descriptive nature.

4.2. Study population and sample:

The study population consisted of all male and female teachers of Palestinian schools in Qatar in the academic year 2021/2022, and they were (60) male and female teachers. The researcher distributed a questionnaire to male and female teachers using the school's e-mail. After 14 days, she collected the electronic responses of male and female teachers. Thus, the study sample amounted to 52 male and female teachers, and table (1) shows the distribution of male and female teachers in the study sample by gender and chronological age level.

The variable	Category	Number	Percentage
Gender	male	25	%44.64
	female	31	%55.36
	total	56	%100
Age	from 20-30	15	%26.78
	from 30-40	36	%64.28
	from 40-50	5	%8.92
	Total	56	%100

Distribution of study sample members according to gender and chronological age

Table No. (1)

Table (1) showed that the number of male and female teachers in the study sample reached (56), representing (100%) of the total number of the study sample, while the number of male teachers in the study sample reached (25), representing (44.64) of the total number of the study sample, while the number of female teachers is (31), with a ratio of (55.36).

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54 Publication Date: 05-10-2023 ISSN: 2706-6495



The study sample was distributed among three age levels as follows: (20-30, 30-40, 40-50) with percentages reaching (26.87%, 64.28%, 8.92) respectively.

4.3. Study tools:

To achieve the objectives of the study and collect the necessary data, the following two tools were used:

1- **Psychological stress scale**: The researcher prepared a psychological stress scale test, following the following steps:

- Reviewing the educational literature related to psychological stress, and reviewing studies that investigated psychological stress, and the researcher benefited from the standards used by Omran (2001) and Al-Asghar (1999) who measured the level of psychological stress.

- Selecting items from the psychological stress scales, rephrasing some of them, and adding items to suit the psychological stress of male and female Palestinian school teachers in Qatar.

- Constructing a psychological stress scale in the form of a tripartite scale, which included the following grading: (I suffer to a severe degree = 3), (I suffer to a slight degree = 2), (I do not suffer from a problem = 1). In its initial form, the scale consisted of (60) items measuring the psychological pressures of male and female teachers.

- Validity of the Psychological Stress Scale

To verify the validity of the Psychological Stress Scale, it was presented to a group of specialists in the field of psychology, to express their opinions about the scale's items, in terms of linguistic wording, representation of the psychological stress items, the comprehensiveness of the psychological stress scale's items, and deletion, addition, or modification of what they see fit. Modification were made in light of the arbitrators' comments, where the wording of some items was modified, so the scale came out consisting of (60) items in its final form. The scale's scores ranged from (60-180) degrees.

- Stability of the Psychological Stress Scale

The stability of the Psychological Stress Scale was verified by applying it to a survey sample of (10) male and female teachers in Palestinian schools and re-application after two weeks, and calculating the Pearson Correlation Coefficient between the two applications. The correlation coefficient between the two applications reached (0.83), and the researcher also calculated the



internal consistency of the psychological stress scale using Cronbach's alpha coefficient, which reached (0.91), and the correlation coefficients of the scale's items with its overall self-esteem ranged between (0.98-0.62).

To judge the level of psychological stress among Palestinian male and female school teachers in Qatar; the scale categories were redistributed from three categories to three categories as follows:

- First: (1.00-1.39) is a small degree.
- Second: (1.40-2.21) average grade.
- Third: (2.22-3.00) high degree.

2- Achievement Motivation Scale:

The Achievement Motivation Scale test was prepared according to the following steps:

Reviewing the educational literature that related to achievement motivation, and then searching the educational literature related to the areas of achievement motivation to learn how to measure it and formulate the paragraphs in their initial form.

Reviewing studies that aimed to measure achievement motivation such as the study of Shaheen (2012) and Al-Qabali (2009), identifying some paragraphs appropriate for the sample of this study, and selecting some paragraphs and reformulating them in a way that suits the objectives of the study and the nature of its sample which consists of university students.

Preparing the scale in its initial form as it included personal information such as gender and academic level. The scale was also prepared so that each item in it corresponds to a five-point (Likert) grading, and the teacher can choose what suits him from it, and the grading included the following: (always = 5, often = 4, sometimes = 3, rarely = 2, never = 1). In its initial form, the scale consisted of (40) items.

-Validity of the Achievement Motivation Scale

The Achievement Motivation Scale was presented in its initial form to a group of specialists in the field of psychology to express their opinions about the items of the scale, in terms of the linguistic wording of the items, their comprehensiveness to measure achievement motivation, and the paragraphs' representation of achievement motivation, with the possibility of modification or deletion or addition.



In light of the arbitrators' comments, the wording of some items was modified, so the scale came out consisting of (40) items in its final form, and the scale scores ranged from (40-200) degrees.

- Stability of the Achievement Motivation Scale

The stability of the Achievement Motivation Scale was verified by applying it to a survey sample consisting of (10) male and female Palestinian school teachers in Qatar .The survey sample was randomly chosen using a simple random method, and it was re-applied to it after two weeks. A correlation coefficient was calculated using Pearson Coefficient between the two applications. The correlation coefficient reached (0.87). The researcher also calculated the internal consistency of the achievement motivation scale using Cronbach's alpha coefficient, and it reached (0.93). The correlation coefficients of the scale's items with its overall skill ranged between (0.97- 0.73).

To judge the level of achievement motivation among teachers on the Palestinian schools in Qatar; the scale categories have been re-distributed from five categories to three categories as follows:

First: (1.00-2.33) is a small degree.Third: (2.34-3.67) average grade.Fourth: (3.68-5.00) high score.

4.4. Study procedures:

The following steps were followed to achieve the objectives of this study:

- 1- Reviewing the educational literature and previous studies that dealt with achievement motivation and psychological stress.
- 2- Building study tools and verifying their validity and reliability.
- 3- Obtaining permission to implement the study from Palestinian schools in Qatar.
- 4- Determining the study sample of male and female Palestinian school teachers in Qatar by the intentionally method.
- 5- Applying the study standards to male and female teachers in Palestinian schools in Qatar.
- 6- Collecting data, transcribing the results into an Excel spreadsheet, and organizing them.
- 7- Processing data via the statistical program (SPSS).



8- Organizing and discussing the results and making recommendations in light of the study results.

4.5. Statistical methods:

To achieve the objectives of the study and process the data collected using the study standards, the following statistical methods were conducted:

- 1- Calculate the Pearson Correlation Coefficient to verify the stability of the measures by applying and re-application.
- 2- Use Cronbach Alpha correlation coefficient to verify the stability of the scales by calculating internal consistency.
- 3- Calculate means and standard deviations to measure the level of achievement motivation and psychological stress among male and female teachers in Palestinian schools in Qatar.

4.6. Study variables:

The study addressed the following variables:

- Achievement motivation
- Psychological pressure.

5. Discussing the results

The results were presented and discussed according to the sequence of questions as follows:

Results of the first question: What is the level of psychological stress among male and female teachers in Palestinian schools in Qatar?

To answer this question, the means and standard deviations were calculated for the study individuals' responses to the psychological stress scale, as shown in Table (2).

Table (2): The arithmetic means and standard deviations of the study individuals' responses to the psychological stress scale

Rank	No.	Item	Mean	Standard deviation	Estimates
1	2	I suffer from my daily school performance in general in light of the Corona crisis	2.61	0.82	High
2	24	I suffer from poor education in scientific subjects in	2.59	0.86	High

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54



Publication Date: 05-10-2023 ISSN: 2706-6495

		light of the Corona crisis.			
3	26	I suffer from low proficiency in the English language	2.57	0.91	High
4	23	I suffer from a weakness in my ability to perform in light of the Corona crisis	2.56	0.87	High
5	25	I forget all or some of what I know	2.56	0.87	High
6	28	I do not have enough desire to teach	2.55	0.88	High
7	5	I do not have a suitable environment to work from home	2.53	0.92	High
8	37	I often feel bored in class	2.52	0.95	High
8	35	I suffer from poor concentration during education	2.52	0.98	High
9	27	It bothers me what some students do to disrupt classes	2.52	0.92	High
10	10	I am struggling to make an assessment for students	2.50	0.95	High
10	3	I find it difficult to ask students questions	2.50	0.90	High
10	17	I don't know how to study in the precautionary atmosphere	2.50	0.91	High
10	4	I suffer from narcolepsy (daydreaming)	2.50	0.85	High
11	15	I suffer from a lot of distraction in class	2.49	0.90	High
11	12	I find it difficult to get along with my co-workers	2.49	1.47	High
12	21	My family does not care about my position abroad	2.48	0.94	High
12	8	My colleagues assign me most of the department's work	2.48	0.94	High
13	1	My boss treats me badly and tries to control me	2.47	0.84	High
13	13	I suffer from the cruelty of the manager in his dealings with me	2.47	0.91	High
14	16	I suffer from frequent quarrels with my colleagues	2.46	0.94	High
14	33	I suffer from respect among my colleagues	2.46	0.96	High
14	9	My boss prefers regardless of my colleagues	2.45	0.96	High

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54



Publication Date: 05-10-2023 ISSN: 2706-6495

15	39	I can't tell my boss about my problems	2.44	0.97	High
15	6	My boss gets involved in picking assignments	2.44	1.02	High
16	22	My boss expects more from me than I can handle	2.43	0.96	High
16	7	I suffer from my manager's interference in my private affairs	2.43	0.96	High
17	34	My relationship with teachers or some of them is bad	2.41	1.08	High
18	20	It bothers me that teachers are unfair in their dealings with students	2.40	0.96	High
19	18	I feel that the teachers do not respect the students	2.38	0.98	High
25	38	I feel like the manager doesn't care about me	2.32	1.12	High
26	29	The boss scolds me and insults me in front of colleagues	2.33	1.14	High
26	30	I'm afraid of the manager	2.33	1.08	High
1	2	I don't have any girlfriends/boyfriends	2.61	0.82	High
2	24	My classmates/colleagues don't like me	2.51	0.86	High
3	26	My classmates/colleagues treat me selfishly	2.57	0.91	High
4	23	I often quarrel with my classmates/colleagues	2.56	0.87	High
5	25	My colleagues/colleagues joke with me	2.57	0.87	High
6	28	My male/female colleagues scold me with profanity	2.55	0.88	High
7	5	My colleagues call me names that I don't like	2.51	0.92	High
8	37	My colleagues do not accept me who disagree with them in opinion	2.52	0.95	High
8	35	My male/female colleagues do not respect my feelings	2.52	0.98	High
9	27	I don't know how to make friends / girlfriends	2.50	0.92	High
10	10	My monthly salary is not enough	2.51	0.95	High
10	3	I do not have the money to buy notebooks and school supplies	2.49	0.90	High

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54 Publication Date: 05-10-2023 ISSN: 2706-6495



10	17	My income is not enough to cover my living expenses	2.49	0.91	High
10	4	I suffer from shyness towards the opposite sex	2.49	0.85	High
11	15	I suffer from being involved in a relationship with the opposite sex	2.48	0.90	High
11	12	I feel depressed and sad often	2.48	1.47	High
12	21	I get shy when I'm in a group	2.47	0.94	High
12	8	It bothers me that I get angry quickly	2.47	0.94	High
13	1	I suffer from insomnia	2.44	0.84	High
13	13	I feel anxious often	2.44	0.91	High
14	16	I get bored often	2.43	0.94	High
14	33	I am afraid of failure in my work	2.43	0.96	High
14	9	I don't know how to express myself clearly	2.44	0.96	High
15	39	My GPA does not qualify me to be promoted to the job I want	2.42	0.97	High
15	6	Our financial capabilities do not enable me to buy more	2.43	1.02	High
16	22	I don't know what to do after I complete my educational mission	2.41	0.96	High
16	7	I have no information about future job opportunities	2.41	0.96	High
	·	Total degree (psychological stress)	2.46	0.55	High

It is clear from Table (3) that the mean of psychological pressures reached (2.46) with a standard deviation of (0.55) with a high degree. It also appears from Table (3) that all items of the psychological pressures scale came with a high degree, and that paragraph No. (1) "I am suffering from the level of my daily school performance in general in light of the Corona crisis." It came in first place with a mean of (2.61) and a standard deviation of (0.82), and paragraph No. (2) "I suffer from a decline in my education in scientific subjects in light of the Corona crisis." It came in second place with a mean of (2.59) and a standard deviation of (0.82).



The researcher attributes this result to the association of psychological stress with the presence of the effects of the new Corona virus which the study is based on, and what it entails in setting hypotheses and testing them to reach a solution to the problem of the study. Samira Muhammad, quotes from Hans Selye and indicates that many environmental factors change the supposed state of balance of the human body, which leads to the body taking various reactions to restore balance. These actions have been called psychological stress or stress triggers, and they include anything that requires the body to mobilize its responses. The body responds to stress with an organized system of physical and chemical variables that help the individual to confront or escape from them.

Also, most female teachers are in a state of psychological stress, and this result can be interpreted according to what Baron et al. (1995) presented, defining psychological pressure as an interactive component that contains three components: environmental needs, individual capabilities, and poor costs that fall between the previous two components. This causes poor adaptation between the individual and the environment around him.

In addition, this result may be attributed to Palestinian teachers in Qatar who have psychological stress, expectations, and goals that change with ongoing circumstances, as every male and female teacher has chosen his or her professional path and specialization.

Results of the second question:

What is the level of achievement motivation among male and female teachers in Palestinian schools in Qatar?

To answer this question, means and standard deviations were calculated for the study individuals' responses on the achievement motivation scale, as shown in Table (3).

Rank	No.	Item	Mean	Standard deviation	estimates
1	15	I feel happy when I complete a task successfully	3.78	0.56	high
2	8	I imagine myself successful	2.55	0.75	middle

 Table (3) Arithmetic means and standard deviations of the study individuals'

 responses on the achievement motivation scale

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54 Publication Date: 05-10-2023 ISSN: 2706-6495



3	14	I struggle to reach my goal	2.85	0.72	middle
4	5	I take responsibility for my actions	3.54	0.76	middle
4	32	I strive to achieve future goals	2.32	0.79	low
5	18	I care about perfecting my work	4.43	0.81	high
6	13	I can encourage myself to achieve my goals	3.44	0.84	middle
7	21	My work results from my desires, not from the desires of others	4.35	0.91	high
7	39	I have competencies and abilities that qualify me to excel	4.35	0.82	high
8	4	I refuse to give up easily	4.33	0.88	high
9	22	I believe that successful people are life creators	4.30	0.99	high
10	31	I believe that what does not break my back makes me stronger	3.35	0.92	middle
11	20	I admit my mistakes as well as my successes	4.24	0.90	high
11	25	I feel anxious and upset because I have not achieved a high level of education	4.24	0.97	high
12	30	I think I'm persistent	3.33	0.93	middle
13	2	I like to be at the forefront of academic achievement	4.21	0.9	high
13	34	I like to listen to success stories	4.21	0.99	high
13	37	I enjoy seeking knowledge and achievement	3.52	0.89	middle
14	23	Stay organized to make implementation easier	3.15	0.96	middle
15	29	I can do special things	3.25	0.88	middle
16	1	I try to outperform my colleagues	3.54	0.95	middle
17	9	When I start something I don't stop until I finish it	3.56	0.91	middle
17	12	Material rewards encourage me to achieve	4.13	1.08	high
18	11	Enjoy competing with others in completing	4.12	1.00	high

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54



Publication Date: 05-10-2023 ISSN: 2706-6495

	т – – –		,		1
		tasks			
19	3	I constantly make plans for my academic future	3.23	0.99	middle
20	10	I feel responsible towards others	4.08	0.99	high
21	27	I try to solve my problems without asking for help	3.26	0.92	middle
22	36	The knowledge I receive at school is very useful to me	4.04	0.98	high
23	38	I am satisfied with my achievements	3.46	1.13	middle
24	17	Not succeeding in a task motivates me to try	3.32	0.98	middle
25	40	Studying at university is fun for me	3.89	1.12	high
26	28	I immerse myself in my work without caring about the financial return	3.32	0.99	middle
27	6	I have had enough independence since I was young	3.85	1.04	high
28	33	I tend to work more than I tend to rest	3.79	1.08	high
29	7	Complete tasks that are difficult for others with ease	3.52	0.90	middle
30	35	I care more about what I accomplish than about grades	3.54	1.13	Flat
31	24	I take my time to learn	3.62	1.84	Medium
32	16	I overcome obstacles easily	3.61	0.89	Medium
33	19	I feel that my current studies are below the level of my academic aspirations	3.55	1.31	Medium
34	26	I do not postpone today's work until tomorrow	3.55	1.03	Medium
	Tota	al degree (Achievement motivation)	3.67	0.44	High

It is clear from Table (3) that the mean for achievement motivation reached (3.67) with a standard deviation of (0.44) with a moderate degree. It also appears from Table (3) that the



majority of the paragraphs came with a moderate degree, and paragraph No. (15) "I feel happy when I complete a task successfully" came in first place with a mean of (3.78) and a standard deviation of (0.56) and a medium score, while paragraph No. (32) "I strive to achieve future goals" ranked last with a low score of (2.32) and a standard deviation of (079).

The researcher attributes this result to the fact that male and female teachers in Palestinian schools in Qatar were affected by psychological stress in light of the Corona crisis. They passed these stages of study and achieved fewer achievements on the educational and functional levels. Therefore, they have an average sense of achievement on the educational and functional levels.

This result may also be attributed to the fact that achievement motivation can be developed by linking psychological pressures in light of the threat of the Corona virus, and they will need knowledge and how to learn in light of the atmosphere of epidemics. Al-Atoum, Alawneh, Jarrah, and Abu Ghazal (2011) indicate that the most important thing that develops achievement motivation in teachers is to link psychological pressures with their needs.

This result can also be explained through Atkinson's theory, which links the teacher's expectation of his performance and his self-awareness of his ability and the resulting results. The teacher went through many years of study and passed them, and reached the stage of mastery of the academic subjects, and his expectations regarding his achievements and success are average in light of the positive Corona crisis.

The tendency or inclination to achieve success is something acquired and can be learned. A teacher who has succeeded in all previous stages may become a successful teacher (Petri and Govern, 2004).

The answer to the third question:

To answer this question, the Pearson correlation coefficient was calculated between the level of psychological stress and achievement motivation among male and female middle school teachers in Qatar, as in Table (4)

Table (4): Pearson correlation coefficient between the level of achievement motivation and psychological stress among male and female teachers in Palestinian schools in Qatar

The variable/Pearson	psychological pressures	Motivation to
correlation coefficient		achieve
Achievement motivation	0.747**	1

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54 Publication Date: 05-10-2023 ISSN: 2706-6495



Statistical significance (Sig)	0.000	0.00
Psychological pressures	1	0.747**
Statistical Significance	0.00	0.000

**Dignified at a significance level ($\alpha = 0.01$)

It is clear from Table (4) that the relationship between psychological stress and achievement motivation is a high and statistically significant inverse relationship, as the Pearson correlation coefficient between them reached (0.747^{**}) .

The researcher may attribute this result to the connection between achievement motivation and psychological stress, as stress reduces the ability of the teacher, male and female, to reach the goals desired, while achievement motivation works to motivate male and female teachers to achieve its predictions of success.

Achievement motivation is also linked to psychological stress, as it is believed that linking the work of male and female teachers to their performance and their self-awareness of their ability and the resulting results develops their achievement motivation, and expectations are not built in the mind of the teacher or perceptions of psychological pressures are built in light of the Corona crisis.

The tendency or inclination to achieve success is something acquired and can be learned. Male and female teachers who have succeeded in all stages of their work have learned success (Petri and Govern, 2004). Therefore, male and female middle school teachers for Palestinians in Qatar have tasted success and plan to continue their success, as they have become Success has acquired experience, and requires careful study to overcome those psychological stress at this stage, which means exercising in a practical way the ability to achieve.

In addition, this result may be attributed to the fact that male and female teachers in Palestinian schools in Qatar have exerted psychological stress due to what Qatar in particular is going through and the world in general in light of the emerging Corona virus crisis, which affects the defense of achievement in light of what is currently happening in the educational process. The researcher indicates that the greater the psychological stress, the more negatively it affects the individual's achievement motivation.



6. Recommendations:

In light of the results of this study, the researcher recommends the following:

1. Stakeholders should adopt methods that enhance achievement motivation and reduce the extent of psychological stress among male and female teachers.

2. Adopting scientific research methods among Palestinian school teachers in Qatar in arriving at knowledge of how to overcome this crisis.

3. Benefiting from the level of achievement motivation among male and female Palestinian school teachers in Qatar and developing this in controlling the psychological stress they are experiencing.

4. Enhancing achievement motivation by providing direct feedback to male and female teachers about their achievements.

7. References

- Abu Jado, Saleh (2011). Educational Psychology. (8th edition), Jordan, Amman: Dar Al Masirah for Publishing, Distribution and Printing.
- 2- Abu Riyash, Hussein, Al-Safi, Abdel-Hakim, Ammor, Omaima and Sharif, Salim (2006).Motivation and emotional intelligence, Dar Al-Fikr, Amman, Jordan
- 3- Al-Asfar, Osama Sayed Abdel-Zaher (1999 AD): "Sources of psychological stress among young athletes, Master's thesis," unpublished, College of Physical Education for Boys, Al-Haram.
- 4- Engler, Barbara (1991). Introduction to personality theories. Translated by Fahd Al-Dulaim, Kingdom of Saudi Arabia: Taif, Dar Al-Harthy for Printing and Publishing.
- 5- Bani Yunus, Muhammad (2001). Psychology of motivation. Jordan, Amman: Dar Al Masirah for printing, publishing and distribution.
- 6- Bou Hamama, Djilali, Abdel Rahim, Anwar, and Al-Shahoumi, Abdullah (2006). Psychology of learning and teaching. Kuwait: Al-Ahlia Publishing and Distribution
- 7- Gamal Abdel Nasser Mohamed Al-Sayed (2001 AD): "Psychological pressures associated with sports competition among young athletes," a comparative developmental study, Master's thesis, College of Physical Education for Boys in Al-Haram.



- 8- Rateb, Osama (1990). Motivations for excellence in sporting activity. Arab Republic of Egypt, Cairo: Dar Al-Fikr Al-Arabi.
- 9- Rashwan, Rabie and Ali, Al-Tayeb (2006). Cognitive psychology: memory and information encoding. Arab Republic of Egypt, Cairo: World of Books.
- 10- Al-Sayed, Gamal Abdel Nasser Muhammad (2001 AD): "Psychological pressures associated with sports competition among young athletes," a comparative developmental study, Master's thesis, College of Physical Education for Boys in Al-Haram.
- 11- Shaheen, Muhammad (2012). The effect of successive formative tests in general science for the ninth grade on academic achievement, achievement motivation, and reflective practices. Al-Aqsa University Journal (Humanities Series). 18(1): 197-227.
- 12- El-Sheshtawy, Mohamed El-Sayed (2000): "A comparative study of professional psychological pressures among male and female physical education teachers in the Central Delta Educational Sector," Master's thesis, Faculty of Physical Education for Boys, Helwan University.
- 13- Al-Safi, Abdullah (2000). Attribution of academic success and failure and its relationship to achievement motivation. Umm Al-Qura University Journal, 12(2): 80-106.
- 14- Al-Safi, Abdullah (2001). School climate and its relationship to achievement motivation and the level of ambition among a sample of male and female secondary school students in the city of Abha. Arabian Gulf Message Journal, (79): 55-66.
- 15- Abdel-Latif Khalifa (1997) A comparative cultural study between Egyptian and Sudanese university students regarding achievement motivation and its relationship to some variables, Journal of Psychology, Year 11, Issue 44.
- 16- Attia, Omar (2002). Achievement motivation among middle and high school students of both sexes: a comparative developmental study. Unpublished master's thesis, Ain Shams University, Cairo, Egypt.
- 17- Alawneh, Shafiq (2004). Motivation (ed.), General Psychology. Edited by Muhammad Al-Rimawi, Jordan, Amman: Dar Al-Masirah for Publishing and Distribution.



- 18- Alawneh, Shafiq (2004). Motivation (ed.), General Psychology. Edited by Muhammad Al-Rimawi, Jordan, Amman: Dar Al-Masirah for Publishing and Distribution.
- 19- Allawi, Muhammad Hassan (1998): Encyclopedia of Psychological Tests for Athletes, Al-Kitab Publishing Center, Cairo.
- 20- Omran, Sabry Ibrahim (2001): "Psychological pressures among athletes in the Arab Republic of Egypt, a comparative study," doctoral dissertation, Faculty of Physical Education, Minya University.
- 21- Omran, Sabry Ibrahim (1996): "A comparative study of psychological stress among some workers in the sports field," unpublished master's thesis, Faculty of Physical Education, Tanta.
- 22- Al-Ghamdi, Ghormallah (2009). Rational thinking, irrational thinking, self-concept, and achievement motivation among a sample of academically excellent and ordinary adolescents in the cities of Mecca and Jeddah. Unpublished doctoral dissertation, Kingdom of Saudi Arabia, Umm Al-Qura University.
- 23- Al-Fahl, Nabil (2000). A study of self-esteem and the reality of achievement among secondary school students in Egypt and Saudi Arabia (a comparative study). Psychology Journal, Egyptian General Book Authority.
- 24- Al-Qabali, Yahya (2009). The effectiveness of an enrichment program based on smart games in developing problem-solving skills and motivation for achievement among outstanding students in Saudi Arabia. Arab Journal for the Development of Excellence.
- 25- Al-Kashef, Ezzat Mahmoud (1991 AD): "Psychological preparation for athletes," Cairo, Dar Al-Fikr Al-Arabi.
- 26- Mustafa, Mr. Abdel Moneim Mohamed (2001 AD): "Psychological stress factors and their relationship to decision-making among referees of sports activities - a comparative analytical study," PhD dissertation, Faculty of Physical Education for Boys, Al-Haram, Helwan University.
- 27- Moussa, Farouk (2003). A test of achievement motivation for children and adults. Arab Republic of Egypt, Cairo: Egyptian Nahda Library.



- 28- Al-Widyan, Hassan (2000). Analysis of students' motivations towards learning swimming according to the SMS model. Field study at Yarmouk University. Mutah Journal for Research and Studies, 15(2).
- 29- Atkinson, J.W. (1960). Achievement motive and test anxiety conceived as a motive approach success and to avoid failure. Journal of Abnormal and Social Psychology, 60. 53-63.
- 30-Ball, S. (1977). Motivation in Education. New York: Academic Press.
- 31- Gok, T. & Silay, I.(2009). The Effects of Problem Solving Strategies on Students' Achievement, Attitude and Motivation. Lat. Am. J. Phys. Educ. 4(1): 7- 21.
- 32-Santrock, J. (2003). Psychology. McGraw Hill, Boston.
- 33-Tarak . Scanlon . Gary l(1990):. stint and Kenneth former elite figure skaters sources of stress
 Journal of sport and Exercise psychology 13, 103 120
- 34- Petri, H, and Govern, J. (2004). Motivation: Theory, Research and Applications. Thomson-Wadsworth, Australia.
- 35-<u>https://blogs.worldbank.org/ar/education/educational-challenges-and-opportunities-covid-19-pandemic</u>
- 36-https://www.who.int/csr/disease/coronavirus_infections/ar
- 37- https://ar.wikipedia.org/wiki

Copyright © 2023 Dr. Dunia Rajeh Moqpil, Professor. Mohamed Jarraya, AJRSP. This is an Open-Access Article Distributed under the Terms of the Creative Commons Attribution License (CC BY NC)

Doi: https://doi.org/10.52132/Ajrsp.e.2023.54.5



Ensuring Environmental Safety through Sustainable Food Safety

Authors:

Aida Esaa Nasser

Senior Food safety specialist, Dubai Municipality, United Arab Emirates

Email: aida-nasser@hotmail.com

Khalid Abdulla Ghloom

Deputy of Food studies and policies section, Dubai Municipality, United Arab Emirates

Abstract:

The Food Safety Management, represented by the section of Food Studies and Policies, in Dubai Municipality the application of best practices in food control, whether imported through land, sea, or air entry points in the emirate of Dubai or produced locally within the country. This is achieved by implementing approved control systems to ensure the sources of food comply with technical regulations, standard specifications, and approved health conditions. Necessary measures are taken to ensure their suitability for human consumption and to maintain the health and safety of consumers in the emirate.

One of the main operations in the section of Food Studies and Policies is assessing and analyzing food-related risks. To excellently achieve the strategic objectives of the Dubai Municipality, it was necessary to develop a sustainable program, including conducting food-related studies and surveys, such as examining non-compliant chemical and microbial contaminants and monitoring them to ensure the sustainability of the safety and quality of food circulating among individuals, contributing to the sustainability of cities and communities.

In this research, we present a collection of local studies in the emirate of Dubai in the field of food safety, which has contributed to providing a scientific model to sustain the health of the community by providing safe and sustainable food.

Keywords: Food sustainability, sustainable food systems, community health.



1. Introduction

In alignment with the vision of Dubai's leaders to become an advanced and pioneering nation, with a focus on individual development through an effective government that embraces innovation, enhances its government performance, and develops its natural and governmental resources, Dubai Municipality, through its Food Safety Department, has recently launched initiatives related to the safety of food products in the local markets. These initiatives aim to enrich scientific studies and research, building a comprehensive government system based on the best global practices in government work. This is intended to encourage various government entities and employees to excel in the nation.

These initiatives in food safety seek to develop and understand the relationship between food and public health. They aim to uncover the scientific, technical, managerial, policy, and legislative factors that impact not only food security but also the safety and health of the community. Dubai Municipality's Food Safety Department has developed an integrated plan to ensure the provision of safe food to improve the health of the UAE community. The overarching goal of these initiatives is to provide sustainable, high-quality, safe food and establish a scientific knowledge base for nutrition and food.

It's well-known that safe food saves lives with every bite consumed by individuals. Billions of people are exposed to risks annually, millions fall ill, and many die due to the consumption of unsafe food. Organizations and governments play a crucial role in ensuring food safety and quality. The initiatives and programs of Dubai Municipality's Food Safety Department aim to provide all stakeholders in food safety with information to alert relevant regulatory authorities to the health risks associated with consuming contaminated or adulterated food. They also provide a sustainable approach to risk assessment through the creation of a contaminants monitoring program for food, ensuring the trade of safe, contaminant-free food that positively impacts the community.

In the future, Dubai Municipality, represented by its Food Safety Department, intends to invest in and further develop the studies conducted in the field of food safety monitoring to achieve even better outcomes. Ultimately, these food safety assessments serve national interests, and Dubai Municipality hopes to apply the system at the level of the Gulf Cooperation Council states and engage in discussions at international forums such as the Dubai World Food Safety Conference.



1.1. Research Problem and Reasons

In the past, farmers were simply asked to produce more food, but now the focus is not only on production but also on sustainable production. Due to the complex motivations and interrelated processes of urban food systems and their multi-level, remote, cumulative, and often unexpected impacts, there is currently no advanced scientific model for sustainable food systems that promote sustainability goals in the face of urban development and population growth.

The phrase "Safe Food, Safe Community" emphasizes the importance of food safety in protecting human health. Food safety includes various measures and practices to prevent contamination, reduce foodborne disease risks, maintain food quality, and ensure proper handling, preparation, storage, and transportation of food. It also involves ensuring that food products are free from harmful bacteria, viruses, chemicals, and other risks.

By promoting safe food practices, we can reduce the risks of foodborne diseases, which can cause serious health problems, especially among vulnerable populations such as children, the elderly, and those with weakened immune systems. Therefore, it is essential to prioritize food safety in our daily lives, from choosing safe and fresh ingredients to cooking and storing food properly, to ensure the health and safety of ourselves and others.

For the future of our local community and to keep pace with its development, the idea of conducting research in the field of food safety sustainability and its role in continuously preserving community health in sustainable communities has been considered.

1.2. The goal of the research

The goal of the research is to align with the United Nations' Seventeen Sustainable Development Goals, including Sustainable Cities and Communities, established by the UN General Assembly in 2015 and to be achieved by 2030. It also aims to support the United Arab Emirates' national agenda, which aligns with UN goals, by proactively managing operations within government entities to enable making the right choices to improve life sustainably for future generations and provide clear principles and objectives for all countries, local governments, and global governments to adopt according to their priorities and national plans.

The Sustainable Development Goals are interconnected, and success in achieving a specific goal in addressing a particular issue often leads to the achievement of other goals. In this research, the focus is on making cities and communities sustainable by achieving comprehensive health

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54 Publication Date: 05-10-2023 ISSN: 2706-6495



coverage, including protection from food contaminants, to ensure the health and sustainability of food supplies in urban and rural communities.

1.3. The importance of the research

The importance of the research lies in proposing a local model that reflects the comprehensiveness of sustainable healthy food and can be applied by organizations and countries. It emphasizes that no country can achieve social and economic growth solely within its borders, highlighting the need for cooperation among nations to achieve global goals and sustainability.

1.4. Questions about the research topic include:

- Is there a definition for methods of food production, distribution, and consumption?

- Do sustainable cities and communities require a safe and healthy sustainable food system?

- Have the necessary services been provided to enable consumers to make informed and responsible food choices in a smooth and sustainable manner?

- Is there a local or global policy to create a thriving economy by providing employment opportunities and labor in the field of sustainable healthy food to contribute to the development of cities and communities?

- Is there an innovation center and a testing platform where companies can develop, showcase, and implement new sustainable food technologies that can be scaled up to improve our food systems?

1.5. The hypotheses include:

- Scientific studies and research in food safety and sustainability may have developed strategies or redefined food systems, such as production and consumption, in response to changing global conditions.

- A safe, healthy, and sustainable food system can encompass the comprehensiveness of sustainable cities and communities.

- There are direct and indirect services to empower individuals in the community to live healthier lifestyles and make more sustainable food choices.

- Local economies are expected to diversify their sources to rely on local resources to support food security.


- International organizations and entities related to human health and the surrounding environment launch global initiatives and programs that include a roadmap for implementing sustainability for private and government entities and community members.

1.6. Study Terminology

Food: Any substance or part thereof, whether raw or primary, or manufactured, intended for human consumption by eating or drinking, including beverages, bottled drinking water, pickles, spices, and chewing gum, and any substance used in the manufacture, preparation, and processing of food, except for cosmetics, tobacco, or substances used only as medicines. (Federal Law No. (10) of 2015 on Food Safety, United Arab Emirates).

Consumer: Anyone who uses food to satisfy their personal needs or the needs of others. (Federal Law No. (10) of 2015 on Food Safety, United Arab Emirates).

Food Safety: Ensuring that food does not cause harm to the consumer when traded or consumed for its intended use. (Federal Law No. (10) of 2015 on Food Safety, United Arab Emirates).

Technical Regulation: A document specifying the characteristics of a service or product, production methods, management systems, terminology, symbols, data, packaging, labeling, and requirements for the declaration of conformity applicable to the product or its production methods or limited to any of them and which conformity with it is mandatory, according to the specifications and standards applicable in the country. (Federal Law No. (10) of 2015 on Food Safety, United Arab Emirates).

Control: A mandatory regulatory activity aimed at protecting consumer health, ensuring the safety of food and feed at all stages of their circulation at any stage of the food chain, and ensuring their compliance with health and quality requirements, and their precise and clear labeling, in accordance with the provisions of this Law and the regulations and decisions issued. (Federal Law No. (10) of 2015 on Food Safety, United Arab Emirates).

Food Safety Systems: Organized scientific methods and approaches aimed at identifying in advance the sources of hazards, assessing them, and taking control measures to ensure food safety. (Federal Law No. (10) of 2015 on Food Safety, United Arab Emirates).

Risks: The possibility of negative effects on human health due to exposure to a hazard source in food or feed at any stage of the food chain. (Federal Law No. (10) of 2015 on Food Safety, United Arab Emirates).



Pests: Living organisms that cause harm.

Contaminants: Any component or substance not primarily added to food and present in it as a result of production processes (including processes that occur during crop growth or animal and bird breeding and veterinary treatments), manufacturing, preparation, processing, handling, packaging, transportation, or trading of this food as a result of exposure to environmental contaminants. (UAE GSO-CAC-107-2007-A Standard for Data Sheet for Food Additives When Sold Individually).

Food Security: Available when all people, at all times, have physical, social, and economic access to sufficient, safe, and nutritious food to meet their dietary needs and food preferences for an active and healthy life. Based on this definition, four dimensions of food security can be identified: food availability, economic and physical access to food, food utilization, and stability over time (Food and Agriculture Organization, 1996, 2009).

Sustainable Food Systems: Preventative food systems that respect biological diversity and ecological systems, are culturally acceptable, accessible, economically fair and affordable, nutritionally adequate, safe, and healthy, while enhancing natural and human resources (Food and Agriculture Organization, 2012).

Sustainable Food System: Provides food security and nutrition for all in such a way that the economic, social, and environmental bases that generate food security and nutrition for future generations are not compromised (High-Level Panel of Experts on Food Security and Nutrition, 2014). The sustainable food system can feed the world and nourish it using the fewest possible resources while improving the availability and accessibility of food resources and their use over time.

Sustainable Development: Sustainable development is defined as development that meets the needs of the present without compromising the ability of future generations to meet their own needs. Sustainable development calls for concerted efforts to build a future for people and the planet that is inclusive, sustainable, and resilient.

The eradication of poverty in all its forms and dimensions is an indispensable requirement for sustainable development. To achieve this goal, it is necessary to promote sustainable, inclusive, and equitable economic growth, create more opportunities for all, reduce inequality, raise basic



living standards, promote fair and social inclusion, enhance integrated and sustainable natural resource management, and improve resource efficiency (United Nations).

Sustainability in the United Arab Emirates: The United Arab Emirates has a rich record in sustainability through pioneering initiatives and projects that reflect the strong values of environmental conservation, social traditions, and other authentic heritage values.

The UAE government has implemented many policies and practices to promote sustainable development at both local and global levels.

After decades of progress and development, the country takes a collective approach to achieving a sustainable future through various initiatives and achievements in many areas and sectors, including supporting initiatives to achieve climate neutrality and enhancing efforts to preserve wildlife and marine life (Sustainable UAE).

2. Previous Studies

2.1. Studies and research on the sustainability of food systems and the sustainability of cities and communities.

United Nations System Standing Committee on Nutrition (2017), Title: Sustainable dietary patterns for healthy people and planet

Within this discussion document affiliated with the Institute of Environment and Sustainability at the University of California, Los Angeles, the term "sustainable dietary patterns" was mentioned. It was concluded that sustainable and healthy dietary patterns can bring mutual benefits for the environment, people's well-being, and their nutritional status. It is essential to integrate nutritional considerations into the climate change agenda. The international government body concerned with climate change also emphasized the shared benefits of measures that reduce climate-altering emissions while simultaneously improving health.

International Livestock Research Institute and Research Program on Agriculture for Nutrition and Health (2017), Title: Food Safety and Sustainable Development Goals.

This brief was prepared by the International Food Policy Research Institute and is derived from previous studies on food safety in developing countries. The brief states that food safety is an integral part of food security and a priority for sustainable development. It is time for food safety to be included in the sustainable development agenda. The brief provides examples of foodborne diseases such as cholera and aflatoxins, which pose risks to food safety. It also discusses how food

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54 Publication Date: 05-10-2023 ISSN: 2706-6495



safety can contribute to achieving sustainable development goals, both directly and through its link to other factors required for goal attainment and improvement. Finally, it examines challenges and concerns that impact goal achievement.

agr.gc.ca (2017), Title: Sustainable Development Strategy at the Departmental Level 2017-2020.

This strategy describes the objectives and plans of agriculture and agricultural food in Canada for sustainable development according to its jurisdiction. It outlines the department's vision and decision-making process for sustainable development, specifies its contribution to achieving the goals of the federal sustainable development strategy, and discusses the application of strategic environmental assessments.

science.gc.ca (2023), Title: Northern Contaminants Program.

The Northern Contaminants Program (NCP) was established in 1991 in response to concerns about human exposure to high levels of contaminants in wildlife species vital to the traditional diets of northern Indigenous peoples. Recent studies have found a wide range of substances, many with no sources in the Arctic or Canada, yet they have unexpectedly reached high levels in the northern ecosystem.

The goal is to reduce contaminants in traditionally harvested foods and eliminate them where possible while providing information to help individuals and communities make informed decisions about their food use.

European Union (2023), Title: Sustainable Food Systems.

This brief presents a pre-legislative synthesis of national and regional government organization positions on the upcoming proposal by the European Commission regarding sustainable food systems. It provides a summary of the pre-legislative state and pre-consultation on a set of key priorities of the European Commission and a study on the functioning of current policy and identifies best practices and ideas for the future.

The brief concludes that policy issues related to sustainable food systems are multifaceted and interconnected, with sustainability being a priority goal in a wide range of national, regional, and local government policies, alongside environmental measures. More of these measures are expected to be implemented in the near future.



2.2. Previous local studies related to pesticide residues in food products.

Dubai Municipality (2021), Title: Pesticide Residue Results in Imported Rice Varieties Available in the Local Market of Dubai.

In this study, the Food Studies and Policies section of Dubai Municipality presents the results of the analysis of pesticide residues in food products in the local market, including Basmati rice, according to the technical regulations set by the Emirates Authority for Standardization and Metrology for maximum allowable pesticide residues and the residual concentration in agricultural and food products. The results analyzed raise concerns about consumer health, and the study proposes several recommendations to enhance the efficiency of control systems by the relevant regulatory authorities to address pesticide residue exceedances in rice.

Ajman Journal of Studies and Research (2022), Title: Pesticide Residue Results in Imported Grains, Pulses, Seeds, and Nuts through Dubai Emirate Port and the Local Market of Dubai. Another study, conducted by the Food Safety Studies and Policies section of Dubai Municipality, presents the results of pesticide residue analysis in food products in the local market, including grains, pulses, seeds, and imported nuts, according to the technical regulations specified by the Emirates Authority for Standardization and Metrology (UAE.S MRL 1: 2017). The analysis is based on monitoring activities conducted by the Food Safety Department, and the study identifies non-compliant varieties with pesticide residue standards in agricultural and food products.

elsevier.com (2022), Title: Pesticide Residues in Fresh Vegetables Imported to the UAE.

This study highlights the significant increase in the use of pesticides in many countries, with excessive use having potentially harmful effects on health and the environment. The study evaluates pesticide residues in vegetable samples that entered the United Arab Emirates through Dubai Emirate ports in 2018 and 2019. The monitoring results are based on Maximum Residue Limits (MRLs) set by the European Union regulations for each pesticide in each product, revealing residues exceeding the maximum allowable limits.

2.3. Discussion of Previous Study Results:

The studies presented in this research show various activities carried out by countries, organizations, and health authorities related to food control. These activities include strategies, policies, research, studies, and recommendations that improve people's lives in multiple ways, from addressing diet-related diseases to supporting startups and building stronger communities

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54 Publication Date: 05-10-2023 ISSN: 2706-6495



while protecting the environment. These efforts by government and non-governmental organizations contribute to creating a sustainable food environment for society.

At the local level, particularly within the Food Safety Department, there are scientific studies stemming from annual surveys that focus on assessing the presence of chemical residues, such as pesticide residues, in food and agricultural products and their impact on human health and the environment. This extends the work of the Food Studies and Policies Department's programs for monitoring and controlling pesticide residues in food, aiming to assess the contamination of food with pesticides, identify the most contaminated food types and sources, and detect the use of unregistered and prohibited pesticides in imported foods, ultimately reducing pesticide residues in food products.

3. Research Strategy and Methodology:

The research objectives were achieved through strategies including:

1. Descriptive/Qualitative Strategies: To highlight the research topic, describe and identify the phenomenon or problem, and establish the relationship between environmental sustainability, food sustainability in communities, and their impact on consumer health.

2. Qualitative Strategy: To define the research goal, which is the sustainability of cities and communities, in line with the United Nations 2030 agenda.

3.1. Research Sources:

- Library Sources: Relevant books related to the research topic were consulted, along with scientific studies published in Arabic and foreign journals.

- Electronic Sources: These included websites, research reports, scientific journals, as well as official government publications from ministries and relevant entities related to the research topic. Data and information from the Food Safety Department at Dubai Municipality were also included.

3.2. Data Processing:

The available data consisted of a plan for food sample surveys, which encompassed the expected food contaminants in products available for trade in the local market.

3.3. Study Boundaries:

- Temporal Boundary: This involved presenting a model of the annual survey plan in the Food Studies and Policies section of the Food Safety Management over the past years.



- Field Boundary: The survey plan included collecting food samples for laboratory analysis from various geographical locations in Dubai's food establishments to ensure the safety and quality of food and drinking water, as well as animal products.

Food Surveillance Plan in the Emirate of Dubai

The implementation of surveys and field studies, as well as the collection of samples for analysis, to ensure the safety and quality of food, drinking water, and traded animal products.

Food Safety Management primarily relies on accredited local laboratories to perform chemical and biological examinations on food and drinking water samples to determine their compliance with relevant specifications and technical regulations.

The steps of the food surveillance plan in Food Safety Management are as follows:

- Study and evaluate food contaminants within a survey card model. This card explains the reasons for the need for the survey throughout the year, the survey's objectives, sample descriptions, and their quantity.

- Enumerate all the tests that the annual survey plan will cover within one template so that these tests are repeated throughout the year on food products and their various types from different geographic locations."

The relationship between pesticide use in agricultural production and its impact on human health and the environment is overseen by the World Health Organization (WHO) in collaboration with the Food and Agriculture Organization (FAO). They are responsible for assessing the risks of pesticide residues on humans, whether through direct exposure or through residues present in food. They also issue necessary recommendations to ensure protection measures.

A team of international scientific experts, represented in the joint meeting of FAO and WHO, conducts risk assessments specific to pesticide residues in food. These assessments rely on all the data provided at the national level worldwide, as well as peer-reviewed scientific studies published in journals. After risk evaluation, this joint committee establishes safe intake limits to ensure that the levels of pesticide residues people are exposed to through their food consumption over their lifetimes do not have harmful health effects.

These acceptable daily intake levels are used by governments and international risk management bodies, such as the Codex Alimentarius Commission (the international governmental body responsible for food standards), to set maximum limits for pesticide residues in food.

Academic Journal of Research and Scientific Publishing | Vol 5 | Issue 54 Publication Date: 05-10-2023 ISSN: 2706-6495



The Codex Alimentarius standards serve as a reference for food trade at the international level, ensuring consumers everywhere can trust that the food they purchase meets safety and quality standards, regardless of where it was produced. It's worth noting that there are currently standards for over 100 different types of pesticides.

WHO and FAO together have established the International Code of Conduct on Pesticide Management. The latest version of this voluntary framework, published in 2014, guides governmental regulatory bodies, the private sector, civil society, and all stakeholders on best practices in pesticide management throughout their life cycle, from production to disposal.

(Published by the Public Health Organization on February 19, 2018).

Impact of Pesticides on Humans, Water, Soil, and Air:

Pesticides can enter the human body through various means, including the respiratory system, skin, and, most commonly, food consumption. They accumulate in human tissues and can disrupt cell division, leading to genetic changes and affecting organs like the liver, which plays a significant role in bodily functions.

Pesticides also play a crucial and significant role in contaminating water and soil. Pesticides can settle on the soil surface during spraying operations, becoming a source of water pollution. Heavy rainfall after spraying can accelerate pesticide movement into soil particles and, subsequently, into the aquatic environment. The extensive use of pesticides in agriculture has led to contamination of water bodies and, in some cases, groundwater.

Pesticides can impact soil by disrupting the formation of nitrogen-fixing bacterial nodules, upsetting the balance of soil organisms.

Furthermore, pesticides can affect air quality, potentially harming human, animal, and plant health and their activities in the environment.

In summary, the environment, including land, water, and air, is exposed to chemical residues, including pesticides used in agriculture. These residues can accumulate in the environment over the long term, affecting environmental sustainability and communities.

This research has reversed a local model by providing a practical model that contributes to supporting local food systems and preserving food safety by examining pollutants in locally traded foods annually. This ensures the provision of safe and healthy food to the community. However, this program also has broader implications at both the local and global levels.



For example, when monitoring the results of pollutant surveys in food, it was observed that there were positive results for certain chemical pollutants, such as pesticide residues, exceeding the allowed limits for food production according to local and international regulations. This has implications for human health in the community in the short and long term, as well as potential effects on the environment due to random use by producers (farmers).

The Food Safety Department in Dubai Municipality has taken a positive and radical step in addressing food and environmental issues by collaborating with local federal authorities responsible for health and environment matters. They also engage with importing countries of food products that do not meet regulations and specifications, discussing issues that threaten human health and the environment, including pesticide residues in imported foods, and addressing this challenge at both the local and global levels.

4. Research Results

The research has yielded numerous results that can be utilized in sustaining food and a healthy environment, contributing to the goal of urban and community sustainability.

Firstly, the research addressed topics and proposals that answer questions and hypotheses at the beginning of the study. There are guidelines for a sustainable approach to food consumption that assist in raising sustainability indicators, including environmental and community sustainability in cities.

Secondly, based on previous research and studies discussed in this research, there are initiatives and programs in food systems, both at the local level in specific countries and as systems established by health-related organizations concerned with food safety, the environment, and sustainability. Each entity prioritizes taking steps towards food system sustainability, creating roadmaps to achieve this goal, providing solutions to challenges, addressing issues related to food, environment, public health, and striving to establish comprehensive infrastructure and systems covering all sustainability goals globally.

Thirdly, at the local level in the Emirate of Dubai, global practices in food safety and regulation have been adopted, which, in turn, play a crucial role in other areas, including individual health and the surrounding environment. This is part of Dubai's vision and strategy for implementing sustainability across various sectors, including the implementation of a sustainable program serving local food systems, particularly in monitoring food pollutants.



Fourthly, the study highlighted random practices by farmers and food producers in the misuse of pesticides without following recommended instructions from pesticide manufacturers. This may be due to a mistaken belief among farmers that adding more pesticides is effective in increasing production. This is related to the cultural level of farmers in certain countries. Also, the use of pesticides in developing countries facing food crises is attributed to the lack of awareness and regulation by exporting countries, and as a result, these improper practices have a significant impact on the environment and its sustainability.

5. Recommendations:

- Develop and implement a standardized model for sustainable food systems at the local and federal levels.

- Prepare a local guide (Sustainable Healthy Markets) to achieve sustainable food systems by all members of society, food producers, consumers, and responsible authorities.

- Transition to a sustainable society by building a strong vibrant community, one of the pillars of achieving the vision of the United Arab Emirates, by developing strategies and policies for the urban food system and its sustainability. Promote sustainable urban expansion through community reliance on local resources and sustainable provision of local production (food security) for future generations.

- Enact laws and regulations that align with the sustainability of cities and communities.

- Develop and innovate a comprehensive system for food, environment, and public health sustainability.

- Encourage participation in the innovation of sustainable health systems.

- Implement local scientific studies and research in the field of sustainable health systems.

- Governmental and leadership excellence in creating jobs and services that enhance the sustainability journey.

6. References

- Agriculture and Agri-Food Canada, (2017), Departmental Sustainable Development Strategy www.agr.gc.ca
- Aida Nasser and others, (2021), Results of pesticide residues in imported rice varieties available in Dubai local market, Dubai Municipality.



- Aida Nasser, (2022), Results of pesticide residues in the varieties of grains, legumes, seeds and nuts imported through Emirate of Dubai and collected from Dubai local market, Ojman Journal of Studies and Research pality.

- Northern Contaminants Program, (2023), <u>https://science.gc.ca/site/science/en/northern-contaminants-program</u>
- Professor peter, (2017), Food safety and the Sustainable Development Goals ILRI (GCIAR) research center.
- Tareq M.Osaili and others, (2022), Pesticide residues in fresh vegetables imported into the United Arab Emirates, ScienceDirect.
- Siemen van Berkum, (2018), The food systems approach sustainable solutions for a sufficient supply of healthy food, Wageningen Economic Research.
- Sustainable Development, (2015), World Health Organization Framework Convention on Tobacco Control (United Nations, Treaty Series, vol. 2302, No. 41032).
- United Nations, Transforming our world: the 2030 Agenda for
- Vasilis Margaras and Antonio Albaladejo Román, (2023), Sustainable food systems, Giulia De Nardin Linking the Levels Unit and Members' Research Service.

Copyright © 2023 Aida Esaa Nasser, Khalid Abdulla Ghloom, AJRSP. This is an Open-Access Article Distributed under the Terms of the Creative Commons Attribution License (CC BY NC) **Doi:** <u>https://doi.org/10.52132/Ajrsp.e.2023.54.6</u>