INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 13, Issue 11, (2023) E-ISSN: 2222-6990

Incorporating Fraud Risk Management into the Fabric of Sustainable Digital Business Operations: Post Pandemic Era

[1]Emmanuel Lumbwe, [2]Asif Mahbub Karim and [3]Joseph Adaikalam

[1]PhD Researcher, Binary University, Malaysia, [2]Professor & Dean, Binary Graduate School, Binary University, Malaysia, [3]Founder and Executive Chairman, Binary University of Management & Entrepreneurship, Malaysia.

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v13-i11/19682 DOI:10.6007/IJARBSS/v13-i11/19682

Published Date: 21-11-2023

Abstract

In the aftermath of the pandemic, businesses have expedited their digitalization journey, focusing on sustainability as a fundamental tenet of their operations. This abstract delves into the vital need for seamlessly weaving fraud risk management into the tapestry of sustainable digital business operations during the post-pandemic era. As companies pivot towards digitized landscapes, their susceptibility to a gamut of fraudulent activities heightens. This abstract accentuates the significance of an all-encompassing strategy that aligns fraud risk management harmoniously with sustainable business paradigms. By amalgamating these two critical facets, enterprises can shield not only their financial interests but also proactively contribute to the greater societal and environmental good. Furthermore, this abstract casts light on the shifting panorama of fraud risks, spanning cyber incursions, identity usurpation, and online swindles, which surged amid the pandemic. It underscores that entrenching fraud resilience within digital strategies augments an organization's capacity to adeptly navigate unforeseen disruptions. The abstract also underscores the pivotal role played by technological catalysts like artificial intelligence, machine learning, and block chain in bolstering fraud detection and prevention mechanisms. Harnessing these tools not only enhances operational efficiency but also reinforces the credibility of sustainable practices. In summation, this abstract encapsulates the crux of assimilating fraud risk management into the nucleus of sustainable digital business operations. By adopting this symbiotic approach, businesses can adeptly manoeuvre the intricacies of the post-pandemic terrain while propelling their dedication to both fiscal prosperity and societal conscientiousness.

Keywords: Fraud Risk Management, Sustainable Operations, Digital Business, Cyber Threats, Ai And Machine Learning, Blockchain, Operational Efficiency.

Introduction

In recent years, the connection of fraud risk management and sustainable business operations has gained cumulative consideration as organizations navigate the dynamic environment of digital business. The year 2020 marked a significant turning point, with the COVID-19 pandemic catalyzing a rapid shift towards digitalization across industries (Hossain et al., 2023). As businesses embraced digital platforms to ensure continuity, the vulnerabilities inherent in digital ecosystems became more pronounced, exposing them to a heightened risk of fraud. The COVID-19 pandemic has further exacerbated this situation, as businesses have had to rapidly transition to digital operations, often without adequate security measures in place. This has underscored the urgent need for businesses to incorporate fraud risk management into the fabric of their operations, to ensure their sustainability in the post-pandemic era (PwC's, n.d.). Concurrently, the importance of sustainable practices in business operations has emerged as a critical component for long-term viability and responsible corporate citizenship.

Background

Fraud risk management is a critical aspect of business operations that involves identifying potential sources of fraud, assessing their impact, and implementing measures to mitigate them (ACFE, n.d.). COVID-19 created previously unthinkable consequences for businesses and society. Organized crime has been quick to respond, mounting large scale orchestrated campaigns to defraud businesses, preying on fear and anxiety related to the pandemic (KPMG, 2022).

The period from 2020 to 2023 has witnessed a series of incidents that highlight the necessity of integrating fraud risk management into the fabric of sustainable digital business operations. The digitalization surge that was augmented by the pandemic provoked businesses to reimagine their operations, supply chains, and customer interactions. This change, while suggesting new avenues for expansion and efficiency, also pioneered new paths for fraudsters to exploit weaknesses in digital systems. As indicated in a study by (Bughin et al., 2017) it stated that the advent of the digital era has revolutionized the way businesses operate, offering unprecedented opportunities for growth, innovation, and efficiency However, it has also opened up new avenues for fraud, with cybercriminals exploiting the vulnerabilities of digital systems to commit fraudulent activities (Kshetri, 2015).

Literature from this period point out the need for a proactive attitude to fraud risk management that supports sustainable business practices. Organizations have gradually identified that an effective response to fraud goes beyond safeguarding financial interests; it encompasses protecting brand reputation, maintaining customer trust, and aligning with ethical and environmental imperatives. The COVID-19 pandemic has highlighted the importance of this issue (Hossain et al., 2023). As businesses have had to pivot to digital operations in response to lockdowns and social distancing measures, many found themselves ill-prepared to deal with the increased risk of fraud (McAfee Labs COVID-19 Threats Report, 2020). Cybercriminals have taken advantage of this situation, launching a wave of attacks that have resulted in significant financial losses and reputational damage for many businesses (Mughairi et al., 2019).

In the post-pandemic era, businesses will require to continue operating in a digital environment (Hossain et al., 2023). This makes it imperative for them to integrate fraud risk management into their operations, to protect themselves against the continuing threat of cyber fraud. This will not only help them to safeguard their financial assets and reputation, but also to ensure their long-term sustainability in a progressively digital business landscape.

Problem Statement

The post-pandemic era has seen a significant shift towards digital business operations, which, while offering numerous benefits, also presents a new set of challenges. One of the most pressing issues is the increased risk of fraud in the digital landscape. Despite the growing awareness of this threat, many businesses are still struggling to effectively incorporate fraud risk management into their operations. This lack of effective strategies and measures not only threatens the sustainability of these businesses but also undermines the trust and confidence of consumers and stakeholders (Alshams et al., 2019). Therefore, there is an urgent need to explore and understand how businesses can integrate fraud risk management into their digital operations to ensure their sustainability in the post-pandemic era.

Limitations

The scope of the research is constrained to the post-pandemic era and may not apply to other eras or industries and might not be supported by existing secondary data sources, case studies, and practitioner interviews where possible. Most of the data gathered for the study is qualitative in nature and contains narratives from case studies. The study's concentration on the post-pandemic period might not take into consideration long-term inclinations and deviations in the business environment and the amount of data gathered including the range of businesses to be analyzed may be affected by resource limits, particularly time and financial restrictions. Further research may be necessary to determine the relationship between the integration of fraud risk management and sustainability and particular outcomes. Future research could use a combination of qualitative and quantitative research methods, longitudinal studies, and more diverse samples to achieve a more comprehensive understanding of the integration of fraud risk management and sustainability in digital business operations. Overall, the search results suggest that while there are limitations to the study, it specifies significant insights into the integration of fraud risk management and sustainability within digital business operations. Further research is needed to fully understand the relationship between these factors and their impact on corporate operations.

Literature Review

Fraud Risk Management

The first-ever fraud case dates to 300 BC when two Greek sea merchants Hegestratos and Zenosthemis devised a plan to sink their ship and pocket all the insurance claim loaned money. This is evidence that fraud has been in existence for more than twenty centuries and has in the recent times evolved over the years, going beyond this first recorded instance. Fraud can be defined as deceit with an intent to illegally gain a financial advantage over a person or an entity which two did when the concocted the sinking of the ship.

With the changing landscape over time, fraud has taken different forms, including phishing, credit card and debit card fraud, remote banking fraud, identity theft and identity fraud, advance fee fraud, account takeover, card not present (CNP) fraud, Covid 19 fraud, cyber fraud, and Ponzi schemes or other investment fraud. Some of the most notable fraudsters in history include Charles Ponzi, Bernard Madoff, Sergei Mavrodi, and Victor Lustig. The effects of fraudulent practices are overwhelming, with some of the biggest fraud losses recorded in history being the Enron Corporation scandal and the US paycheck protection program (PPP). The expansion of the internet has created more prospects for fraud, with cybercrime growing to gigantic proportions. Fraud prevention techniques have undergone substantial improvements, with businesses now having several sophisticated tools at their disposal,

including predictive analytics and Artificial Intelligence these have enhanced the fraud risk management over the year (Fraud, 2022).

According to the (Association of Certified Fraud Examiners, 2022) study that examined occupational fraud cases investigated during the period from January 2020 to September 2021. It identifies pandemic-related issues, such as changes in organizational staffing and the transition to remote work, as contributing factors to the frauds investigated. According to the survey contributors, 52% of respondents noted that at least one pandemic-related factor was present in the fraud cases they investigated. The highest common pandemic-related factor was organizational staffing changes, present in 42% of cases. The change to remote work was cited as the most substantial factor in 15% of cases. In terms of specific challenges faced, technology challenges were reported in 12% of cases, supply chain disruptions in 10% of cases, and changes to anti-fraud programs in 11% of cases Operational process changes, internal control changes, shift to remote work, and changes to strategic priorities were also identified as contributing factors (Alkaabi et al., 2020; Jamadar et al., 2021). Overall, the findings suggest that the COVID-19 pandemic has had an impact on occupational fraud, with various pandemic-related factors playing a role in the occurrence of fraud cases.

Among the frequent fraud instances reported were Online fraud, internet fraud instances have escalated as a result of the COVID-19 pandemic's growing reliance on internet transactions. In 2020, there were over 4.7 million reports of fraud reported in the United States, resulting in a $3.3 billion loss overall, according to a report by the Federal Trade Commission (FTC). Comparing this to prior years, there has been a huge increase. A high as more people used the internet to purchase during lockdowns (Hossain et al., 2023), there was a rise in the number of phony websites offering COVID-19-related goods such masks, hand sanitizer, and medical supplies. The victims would make purchases but never get the goods or get fake goods (ACFE Insights, n.d.).

During the epidemic, phishing scams and attacks have also increased in frequency. Cybercriminals frequently targeted on people's worries and apprehensions about COVID-19 to deceive them into disclosing personal information or sending money in an unauthorized manner. The Anti-Phishing Working Group (APWG, 2020) reports that in the first quarter of 2020, there was a 600% rise in phishing assaults related to COVID-19. Prior to the pandemic, identity theft was a problem that persisted, and it has remained so in the post-COVID age. Criminals open phony accounts, make illicit transactions, or file bogus tax returns using stolen personal information, among other sorts of fraud (FTC, 2022)

Government Assistance Fraud increased as several international government assistance programs were put into place as a result of the COVID-19 pandemic. Regrettably, scammers started to target these initiatives. Attempts by individuals and organized groups to cheat government assistance programs, including unemployment insurance (Paycheck Protection Program (PPP) Fraud) or small business loans, Economic Impact Payment (Stimulus Check) Fraud have been documented. Charity fraud was equally noted during the pandemic, a lot of people were eager to give to organizations that supported COVID-19 victims. Fraudsters exploited this goodwill by setting up phony organizations or impersonating actual ones to raise money that was never sent to the intended beneficiaries (FTC, 2022).

The pandemic has led to an increase in fraud cases in the healthcare sector. This includes fake treatments or cures, phony COVID-19 testing, and billing fraud involving medical services. The World Health Organization (WHO) has issued a warning regarding the surge in COVID-19-related healthcare fraud. Further to this, counterfeit medical supplies increased during and after the COVID-19 pandemic that included but not limited to Fake N95 masks, Substandard gloves, Counterfeit test kits and hand sanitizers was noted, putting healthcare workers and

the public at risk of exposure to viruses and bacteria. Inaccurate results due to incorrect diagnoses impacted public health efforts to control the spread of the virus.
Payroll fraud and worker misconduct was noted at some stage in and post the COVID-19 era. Notable was Ghost employees, with remote work becoming more prevalent, some dishonest personnel created fictitious personnel on the payroll and divert their salaries to their personal accounts. Another scheme noted was Time theft, where employees working remotely where falsely reporting their working hours or claiming time beyond regulation hours that they did now not actually work.
Travel and Vacation Scams was on the high with travel restrictions in place, scammers centred persons searching to e book holidays or flights for the future. They would provide pleasing offers or pretend tour packages, taking price however by no means handing over the promised services.
Fraud statistics change rapidly, and new kinds of fraud emerge as criminals adapt to changing circumstances (Ong et al., 2022). To remain knowledgeable about the today's fraud tendencies and statistics, the researcher will proceed to use legitimate sources such as authorities' agencies, regulation enforcement organizations, or research establishments that specialize in fraud prevention and detection.

Sustainable Operations

Andersen (2019); Hossain et al (2022) describes Sustainable operations management (SOM) and strategy as the procedures, processes, practices and systems through which firms—individually or organized in wider inter-organizational structures—initiate, create and deliver outputs that are both profitable from a business perspective, using the resources at their disposal while at the same time taking preservation or even improvement of the natural and/or social environment into account. This builds on the recognition, that companies must also take sustainability issues into account in order to ensure long-term success and survival has he quotes (Hossain et al., 2022; Hart, 2005; Starik et al., 2017).
COVID-19 pandemic brought significant changes in the way businesses operate World-wide (Hossain et al., 2020). Sustainability has become an even more important aspect of business operations (Ariful et al., 2023; Hossain et al., 2022).
The pandemic has shown that remote work and flexible schedules is not only possible but also beneficial to the businesses productivity and improve work-life balance for employees. Though Wang et al (2021); Hossain et al (2018) identified challenges and factors that affect remote workers' performance and well-being is influence by issues such work characteristics which is the nature of the whole job, and scholars do not distinguish offsite and onsite work. Work characteristics can be moderating, mediating, or antecedents in the context of remote work. The study further notes that monitoring in remote work can help remote workers to cope with procrastination and to concentrate on their core tasks. However, monitoring can also increase work-home interference and undermine employee well-being. With regards workload it found that this influences remote workers' work-home balance and can increase their working time (Saleh et al., 2023; Javed et al., 2020). Low workload means more opportunities to procrastinate. Social support was noted to be a powerful virtual work characteristic that helps remote workers to deal with challenges in remote working. Social support can help remote workers to overcome social isolation and reduce psychological strain. Job autonomy is beneficial for work-family balance. Remote workers can control the rhythms of work and rest and have more time to spend with their family.
The search results suggest that the pandemic has accelerated digital transformation and highlighted the importance of sustainability and resilience in business operations. Businesses

have leveraged digital tools and platforms to streamline operations and reduce waste. The pandemic has exposed vulnerabilities in global supply chains, leading businesses to focus on building more resilient and sustainable supply chains. The post-pandemic era presents an opportunity for businesses to transition towards more sustainable and circular practices, such as recycling, reusing, and refurbishing products. Improved stakeholder engagement and transparency efforts are needed to communicate sustainability initiatives and progress (Hossain et al., 2022).

However, according to Sarkis et al (2020) the study identified several challenges that businesses and industries faced in transitioning to sustainable supply and production in response to the COVID-19 pandemic. That the pandemic impelled and was likely continue to drive a global economic catastrophe, and that deep and pervasive societal changes were likely to unfold in the coming months and years. However, he identifies that the pandemic presents an opportunity for accelerating sustainability transitions in the aftermath of the crisis with predictions of social innovations, and technology resulting from the coronavirus outbreak.

The study advised that businesses and industries need to re-examine globalized systems of production based on complex value chains and the international shipment of billions of components and likely prompt establishment of new relationships and supply configurations. Businesses and industries need to re-examine the reliance on just-in-time (JIT) and lean practices and consider alternative supply chain models. Businesses and industries need to manage inventories of essential items in the months and years ahead by having larger supplies on hand and facilities for storage. Businesses and industries need to use state-of-the-art information monitoring, sharing, and prediction capabilities to address points of gridlock in supply chains.

Apart from ensuring business stability, Fraud risks had increased significantly during the crisis, and some businesses may have resorted to unethical practices to avoid portraying a deteriorating financial performance (Vučković et al., 2022; Nur-Al-Ahad et al., 2022). Furthermore, the disruptions caused by the pandemic have created an environment that is conducive to fraudulent financial reporting (Jamadar et al., 2022).

During times of crisis, such as the COVID-19 pandemic, businesses face increased financial losses and uncertainty. These disruptions included rising unemployment, financial losses, and the potential collapse of the capital market. These disruptions created a fertile ground for fraudulent financial reporting and activities to show a more favourable financial position and secure their survival in a challenging market. In order to address this issue and promote business stability, sustainability, and growth, the study suggested one approach was to implement technology solutions, such as fraud detection software, biometric authentication, and encryption. These technologies can help prevent fraud by detecting anomalies and securing sensitive financial data.

Research has shown that controls can be implemented as noted in (Elkhwesky et al., 2022) study which identified some crucial practices that businesses should adopt to prevent fraud and ensure business survival post-COVID-19. Implementing robust internal controls to prevent fraud, these should include segregation of duties, regular audits, and monitoring of financial transactions. Training employees on fraud prevention to help in identifying fraudulent activities, reporting suspicious activities, and the consequences of fraudulent behaviour. Conducting background checks on their employees to ensure that they have no history of fraudulent activities. Implementing technology solutions such as fraud detection software, biometric authentication, and encryption to prevent fraud. Partnering with reputable vendors to ensure that they are not involved in fraudulent activities. Monitoring financial statements regularly to detect any fraudulent activities. Encouraging whistleblowing

for employees to report any fraudulent activities without fear of retaliation. By adopting these sustainable practices, businesses can prevent fraud and ensure business survival post-COVID-19.
Overall, the post-COVID era presents an opportunity for businesses to rethink and transform their operations towards a more sustainable and resilient future. By incorporating remote work, digital transformation, circular economy principles, and prioritizing employee well-being and stakeholder engagement, sound fraud risk management practices can contribute to a more sustainable and equitable businesses world.

Digital Business
The COVID-19 pandemic had a deep effect on businesses globally, forcing many to adapt to digital technologies to continue operating. To ensure sustainability post-COVID era, digital business has continued to play a central role in determining the future.
Digital business is the process of transforming business models and altering a corporation's products and customer experiences, innovating products that create new value and connecting people with things, insights, and experiences. Businesses become more efficient, agile, and customer-centric by digitizing their operations (Alkaabi et al., 2019). Due to the growing digital ecosystem, there has been a high demand for tech-savvy innovators who are well-equipped to improve business operations, processes, and services.

According to Thomas Ritter and Carsten Lund Pedersen (2020) they suggest that the coronavirus crisis has had a significant impact on business models, particularly in the business-to-business (B2B) context. The authors conducted interviews with eight B2B firms during the lockdown period in March 2020. The firms operated in various industries and had a global footprint. The interviews were conducted via video conference due to travel restrictions.
The study identified changes in customers and value propositions as a result of the crisis. Some firms had adapted their service agreements and postponed preventive maintenance. There is also a belief that video meetings will be used more extensively in the future, while personal meetings may become less frequent. The crisis has also led to changes in capabilities, with some capabilities reduced (e.g., sales due to travel restrictions) and others increasing (e.g., online, Internet of Things, delivery services). Some firms have used the idle sales time as an opportunity to develop capabilities and train the salesforce. The study found that exposure to earlier crises has helped firms develop a "crisis capability" and be better prepared for similar events. The analysis also revealed that some parts of a business model may shift to different types as the crisis continued.
The pandemic augmented the adoption of remote work and virtual collaboration tools. Many companies seized the benefits of remote work, such as reduced costs and increased productivity. As a result, remote work is likely to become more prevalent even after the post pandemic era, with businesses investing in digital infrastructure and tools to support remote teams. It further led to a surge in e-commerce and online shopping as people turned to digital channels for their purchasing needs. This trend is expected to continue, with businesses investing in online platforms, digital marketing, and logistics to cater to the growing demand for online shopping. The above has emphasised the importance of digital transformation for businesses to remain competitive and resilient. Companies may likely continue to invest in digital technologies such as cloud computing, artificial intelligence, and data analytics to streamline operations, enhance customer experiences, and drive innovation.
The innovation drive coupled with the fear of virus transmission in the pandemic period fast-tracked the embracing of contactless and touchless solutions across various industries.

Businesses are probable to continue to invest in technologies such as mobile payments, self-checkout systems, and voice-activated interfaces to provide safer and more convenient experiences for customers in the post pandemic eras. The drive has increased reliance on digital technologies, cybersecurity and data privacy will become even more critical. Businesses will need to invest in robust cybersecurity measures and comply with data protection regulations to safeguard customer data and maintain trust.

The pandemic has highlighted the potential of artificial intelligence and automation in improving efficiency and reducing human contact. Businesses will continue to explore AI-powered solutions for tasks such as customer service, supply chain management, and predictive analytics. The healthcare industry saw a substantial swing towards digital solutions during the pandemic, with the extensive implementation of telemedicine and healthtech applications. These trends are likely to continue, with businesses investing in technologies Alshamsi et al (2019) that enable remote patient monitoring, virtual consultations, and personalized healthcare solutions.

Though the above benefits were noted, the shift also gave rise to an increase in digital business fraud prevalence. As more companies have shifted their operations online, fraudsters had taken advantage of the situation to exploit vulnerabilities and carry out fraudulent activities which I have already discussed in this article. However, one worth mentioning is the Business Email Compromise (BEC): BEC scams involve fraudsters impersonating company executives or suppliers to deceive employees into making unauthorized payments or sharing sensitive information. The pandemic created a perfect environment for BEC scams, as remote work setups may lead to less secure communication channels.

To fight digital business fraud in the post-COVID era, individuals and businesses should remain vigilant, educate themselves about common fraud schemes, and implement robust security measures. It is vital to authenticate the validity of websites, emails, and organizations before sharing any personal or financial information. Additionally, businesses should invest in cybersecurity measures, employee training, and fraud detection systems to mitigate the risk of digital fraud.

In conclusion, the post-COVID era will see digital business becoming the new norm across industries. Businesses will need to embrace digital transformation, invest in digital infrastructure and tools, and prioritize cybersecurity and data privacy to thrive in this new digital landscape.

Cyber Threats

Cyber fraud has become a progressively more predominant problem in the post-COVID world. With the fast digitalization of various sectors and the heightened dependence on online platforms, cybercriminals have found new opportunities to manipulate individuals and organizations.

One of the most widespread types of cyber fraud post-COVID is phishing. Cybercriminals send fraudulent emails or messages that appear to be from trustworthy sources, such as banks, government agencies, or healthcare providers, in an effort to swindle individuals into revealing sensitive information like passwords, credit card details, or social security numbers. These phishing attempts often utilize the fear and uncertainty surrounding the pandemic, using COVID-related subjects to bait targets into clicking on malicious links or downloading malware-infected attachments.

According to Powell (2023), the recent case of MGM Resorts 2023 hack was a social engineering attack launched against the IT support vendor employed by Caesar's

Entertainment by hacking gang Scattered Spider. The hotelier was asked to pays around half of the $30 million ransom to the hackers. Resorts put out a statement saying a “cyber security incident” had affected some of the company’s systems. An investigation into the cyber-attack was launched and the relevant authorities contacted. Guests reported a number of issues with MGM Resorts’ online booking system and casino. Financial services company Moody’s says the cyber-attack may negatively impact MGM’S credit. The company also notes that the cyber security incident highlights “key risks” in MGM’s reliance on technology.

WHO (n.d.) discusses the state of cyber defense and the role of trust within organizations. While many organizations report high levels of trust in their cyber defenses, the data suggests that this trust may be misplaced. There are several factors contributing to this "false-positive of trust". The key findings are:

Trust is a major issue and that more than a third (42%) of information security decision-makers reported a lack of trust as their biggest challenge. 95% do not felt as though senior leadership trusts their security teams to protect their organizations from threats. Trust is often misplaced, as Employees' ability to stop a cyberattack (66%) is trusted more than the ability of the security team to identify and prioritize security gaps (63%), the accuracy of data alerts (59%), the effectiveness of cybersecurity tools and technologies (56%), and the accuracy of threat intelligence data (56%).Communication is key and a lack of communication was the most frequent cause for a loss of trust, as reported by 47% of information security decision-makers. Understanding is critical: While 99% agree that endpoint detection and response (EDR) plays a key role, responses show limited understanding of its full function. About 22% of respondents believe that EDR prevents reinfection and 38% believe all responses can be made with EDR, neither of which are wholly accurate. Outsourcing is popular but needs improvement: 98% of those that do not already outsource their cybersecurity services have (or are considering) plans to do so. However, 89% of IT and security decision-makers say improvement is needed in the transparency between their security teams and security vendors. Multiple security tools aren’t solving the problem: The higher the average number of platforms used, the more cybersecurity incidents organizations have experienced. The number of incidents and the fact that only 24% have MDR show that having the right tools, and not the number of tools, is an important factor in cyber protection.

- Organizations are using multiple security tools but still experiencing many cyber incidents, indicating a lack of proper management and strategy.
- Security leaders do not fully understand the capabilities and limitations of their security technologies.
- There is a lack of transparency between in-house security teams and external providers, despite the growing trend of outsourcing cybersecurity services.
- To truly improve their cyber defenses, organizations need to move beyond assumptions and gain a proper understanding of their security gaps and needs. Working with experienced external partners and implementing effective security monitoring solutions can help build the trust required for true cyber maturity.

Another form of cyber fraud that increased during the pandemic was online shopping scams. With the shutting down of physical stores and the increased dependence on e-commerce, cybercriminals setup bogus online stores or marketplace listings to deceive unsuspicious customers. They advertised popular products at tremendously low prices, only to vanish after receiving payment or delivering counterfeit goods. Additionally, remote work unlocked up new paths for cyber fraud. Many organizations shifted to remote work arrangements, leading to an increased reliance on virtual meetings, cloud storage, and collaboration tools.

Cybercriminals took advantage of this shift by targeting remote workers with phishing attacks, malware, or ransomware. They exploited susceptibilities in home networks or unsecured devices to gain unauthorized access to sensitive company data or hold it hostage for ransom. To shield against cyber fraud post-COVID, individuals and organizations should remain alert and implement strong cybersecurity procedures. This includes regularly updating software and operating systems, using strong and unique passwords, enabling multi-factor authentication, being vigilant of suspicious emails or messages, and educating employees about the latest cyber threats. Additionally, organizations should invest in cybersecurity tools and conduct regular security audits to identify and address any vulnerabilities in their systems. Lallie et al (2021) in there study Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic identified that COVID-19 pandemic has led to unique societal and economic circumstances that are exploited by cyber-criminals and that there has been a significant increase in cyber-attacks during the pandemic, with a common modus operandi being phishing campaigns which direct victims to download a file or access a URL that carries malware. Further, these attacks often leverage media and governmental announcements to increase their success rate, showing a loose correlation between the time of these announcements and subsequent cyber-attack campaigns. The research also highlights the potential implications for global policing, suggesting that law enforcement must ensure it has the capacity to deal with the rise in cyber-crime and that changes to working practices and increased rates of unemployment have led to more people spending time online, potentially increasing the overall risk of cyber-attacks.
In conclusion, the COVID-19 pandemic has brought forth a new era of cyber threats. By identifying the manoeuvres used by cybercriminals, supporting our cybersecurity procedures, and nurturing collaboration between law enforcement and cybersecurity experts, we can navigate these challenging times with resilience and protect ourselves from the perils of cybercrime.

AI and Machine learning

Davenport & Kalakota (2019) gives an account of AI (Artificial Intelligence) and machine learning and indicates its rich history that dates back several decades. This algorithm paved the way for a revolution in the field of neural networks, leading to advancements in machine learning. During the 1990s, techniques like support vector machines and decision trees gained acceptance in machine learning. These algorithms aided computers to learn from data and make predictions or decisions without specific programming. The 2000s saw the development of big data, providing massive amounts of data for guiding machine learning models. This resulted in substantial progress in areas like natural language processing, computer vision, and speech recognition. In recent times, deep learning, a subfield of machine learning, has earned significant interest. The blend of AI and machine learning has led to several applications and progressions across several industries, including healthcare, finance, transportation, and entertainment. As technology continues to advance, AI and machine learning are projected to be fundamental in the role of shaping the future.
AI and machine learning have played a significant role during the COVID-19 pandemic and are expected to continue shaping the post-COVID world. Kwekha-Rashid et al (2021) discussed the use of Disease detection and diagnosis of AI algorithms been used to analyse medical images, such as chest X-rays and CT scans, to aid in the detection and diagnosis of COVID-19. These algorithms can help healthcare professionals quickly identify potential cases and prioritize resources.

Qureshi et al (2023) AI has been employed to accelerate the drug discovery process by studying substantial volumes of information and detecting potential drug that can be used. Machine learning models have been used to calculate the effectiveness of existing drugs against COVID-19, leading to the repurposing of certain medications.AI-powered contact tracing apps have been developed to track the spread of the virus and detect potential hotspots. These apps use machine learning algorithms to analyze location data and notify individuals who may have been near an infected person (Fontes et al., 2022). Awasthi et al (2022) discussed how AI can help optimize the distribution of vaccines by analyzing various factors such as population density, demographics, and infection rates. Machine learning models can assist in prioritizing high-risk individuals and ensuring efficient allocation of limited vaccine supplies. Haleem et al (2021) states that AI-powered chatbots and virtual assistants have been used to provide basic healthcare information, answer queries, and triage patients remotely. Machine learning algorithms can investigate patient data and provide tailored treatment proposals, lowering the drain on healthcare systems. Takefuji (2023) in his Case report on enormous economic losses caused by fraud from Japan to the world indicates that in fraud detection AI algorithms can used analyze huge volumes of information, such as financial transactions and insurance claims, to categorise patterns and irregularities that may signify fraudulent activity. Machine learning models can constantly study and adapt to new fraud patterns, improving detection accuracy over time.AI-powered facial recognition and biometric, with the global rise of eCommerce, there have been breaches in online transactions, causing retailers to be concerned about corporate security. Imposters have increased in number as product sales have increased. Having said that, there are tried-and-true techniques for dealing with impostor risks via identity verification. AI-powered Identity Verification is a critical tool for businesses and financial institutions since it may drastically limit cybercrime attack vectors and stop identity theft (Sanctionscanner, n.d).

In the post-COVID world, AI and machine learning are anticipated to remain playing a critical role in innumerable domains. These technologies can help in predicting and preventing imminent pandemics, improving healthcare delivery, augmenting remote work capabilities, and enabling more efficient supply chain management. However, ethical considerations, data privacy, and algorithmic preconceptions need to be addressed to ensure responsible and equitable use of AI and machine learning technologies.

Blockchain

(Nakamoto, 2008) Blockchain technology was first introduced in 2008 by an anonymous person or group of people using the pseudonym Satoshi Nakamoto. It was initially created as a decentralized ledger to support the digital currency Bitcoin. The concept of blockchain revolves around a distributed and decentralized database that maintains a continuously growing list of records called blocks. Each block contains a timestamp and a link to the previous block, forming a chain of blocks. The primary purpose of blockchain is to provide a secure and transparent method of recording and verifying transactions without the need for intermediaries like banks or governments. Since then, blockchain technology has been adopted in various sectors, including supply chain management, healthcare, voting systems, real estate, and more. Its ability to provide transparency, security, and immutability has made it an attractive solution for industries seeking to enhance efficiency and trust in their operations. There are different types of blockchain, including public, private, and consortium blockchains, each with its own benefits and drawbacks. Blockchain technology is still evolving, and researchers and developers are exploring its potential applications in areas like decentralized finance (DeFi), Internet of Things (IoT), identity management, and more.

(Botha et al., 2023) states that during and post the COVID era, there has been an increase in fraudulent activities related to blockchain technology. Scammers have been taking advantage of the fear and uncertainty surrounding the pandemic by promoting fake investment opportunities related to blockchain technology, using phishing attacks to steal sensitive information, launching fake blockchain projects, manipulating the price of cryptocurrencies, and creating counterfeit COVID-19 test certificates. To protect yourself from blockchain fraud, it is important to exercise caution, be skeptical of investment opportunities, be cautious of unsolicited emails or messages, verify the authenticity of blockchain projects, use secure wallets and exchanges, and stay informed. Blockchain technology itself is not fraudulent, but scammers may exploit its popularity and potential during and post the COVID era.

Operational Efficiency

Operational efficiency refers to an organization's ability to utilize its resources effectively to maximize output and minimize waste. Key factors that contribute to operational efficiency include process optimization, resource allocation, technology utilization, employee engagement, and data-driven decision making. Operational efficiency is crucial for organizations to remain competitive in today's fast-paced business environment. It involves streamlining processes, reducing costs, and improving productivity. By continuously striving to improve processes, allocate resources effectively, leverage technology, engage employees, and make data-driven decisions, organizations can achieve higher productivity, lower costs, and ultimately, greater profitability (Indeed, n.d.).

The COVID-19 pandemic has significantly impacted businesses and forced them to adapt to new operational challenges. However, it has also presented opportunities for organizations to improve their operational efficiency both during and after the pandemic. Here are some key factors to consider:

Remote work has been accelerated by the pandemic, leading to increased operational efficiency. Post-pandemic, organizations can continue to leverage remote work options to optimize their operations (Choudhury, 2020). Remote work can save companies on real estate costs and provide benefits such as enhanced productivity and engagement (Parker et al., 2022). AI can help remote workers automate mundane tasks and streamline workflows for maximum efficiency (IMF, n.d.) Digital Transformation: The pandemic has highlighted the importance of digitalization in business operations. Post-pandemic, organizations should continue to invest in digital transformation to enhance operational efficiency and agility (McKinsey & Company, 2020). Automation and AI: Automation and artificial intelligence (AI) technologies can help streamline operations by reducing manual tasks, improving accuracy, and increasing productivity. Post-pandemic, organizations can further explore automation and AI solutions to optimize their processes and improve efficiency.

Prybylski (n.d.) Supply Chain Resilience: The pandemic exposed vulnerabilities in global supply chains, leading to disruptions and delays. To enhance operational efficiency, businesses should focus on building resilient supply chains by diversifying suppliers, improving visibility, and implementing risk management strategies (Stackpole, 2021). Agile Decision-Making: The pandemic has highlighted the importance of agile decision-making in rapidly changing circumstances. Post-pandemic, businesses should continue to foster a culture of agility and flexibility to respond effectively to future challenges (Tovaglieri, 2021). Employee Well-being: The well-being of employees directly impacts operational efficiency. Post-pandemic, businesses should continue to prioritize employee well-being to maintain productivity and engagement (Nasdaq, 2022). AI and Remote Work: AI can help remote workers automate

mundane tasks and streamline workflows for maximum efficiency. AI is a transformative force that's reshaping the workplace and redefining the meaning of work itself.
The future of work is AI-enhanced and remote. AI is rapidly growing in business and is likely to disrupt industries relying most heavily on knowledge work. AI can revolutionize companies as business leaders continue to integrate the work-from-home model for their employees.
Overall, the COVID-19 era has forced businesses to reconsider their operational strategies and find innovative solutions to sustain efficiency. By leveraging remote work, digital transformation, automation, resilient supply chains, agile decision-making, and employee health, organizations can boost their operational efficiency both during and after the pandemic.

Research Questions

- What are the key fraud risks those digital businesses face in the post-pandemic era?
- How can digital businesses effectively integrate fraud risk management into their sustainable operations?
- What are the best practices for identifying and assessing fraud risks in digital business operations?
- What technological solutions can be implemented to mitigate fraud risks in digital business operations?
- How can digital businesses ensure the ongoing monitoring and detection of fraud risks in their operations?
- What are the potential impacts of fraud on the sustainability and reputation of digital businesses?
- How can digital businesses effectively communicate their fraud risk management efforts to stakeholders?
- What are the regulatory and legal considerations that digital businesses need to be aware of in managing fraud risks?
- What are the challenges and barriers that digital businesses may face in implementing effective fraud risk management practices?
- How can digital businesses measure the effectiveness of their fraud risk management strategies and make necessary improvements?

Research Objectives

i. To examine the Impact of the Pandemic on Digital Business Operations: This research objective intends to analyze how the pandemic has shaped digital businesses, principally in terms of fraud risk.
ii. To Identifying the Types of Fraud Risks in Digital Business Operations: This goal is to identify and classify the various types of fraud risks digital businesses are confronted with in the post-pandemic era.
iii. To investigate the connection between fraud risk management and business sustainability: This goal intends to clarify how fraud risk management strategies might help keep digital enterprises viable in the post-pandemic period.

Research Methodology

Secondary research is a research method that uses data that was collected by someone else. In other words, whenever you conduct research using data that already exists, you are conducting secondary research. On the other hand, any type of research that you undertake

yourself is called primary research. Secondary research can be qualitative or quantitative in nature. It often uses data gathered from published peer-reviewed papers, meta-analyses, or government or private sector databases and datasets (George, 2023)
(Cheong et al., 2023) state that secondary qualitative data analysis can be a powerful method by which to gain insights that primary data analysis cannot offer. In this paper they indicate that there is much literature using primary interview data, but often, the primary data represent either a small sample size or a limited regional pool. Additionally, there often is a lack of continuity or connection between the different primary research in literature, which makes them difficult to combine. Furthermore, it is not always possible for various reasons, such as the safety of interviewees as well as the researchers, to conduct ethnography or first-hand interviews. Depending on the research question, a larger geographical and geopolitical coverage might be required, but there often is insufficient resource, budget, or time for first-hand data collection. To overcome these constraints, this paper proposes a method to use publicly available, online secondary data.
Databases of secondary qualitative data can be found in a variety of forms–whether one is already in a structured format or needs to be built via aggregating various sources. Analysis of such secondary qualitative data has established itself as a credible method for generating knowledge Heaton (2008), particularly in nursing Szabo & Strang (1997), as it removes the obstacle of first-hand data collection and its associated challenges of recruitment, and the burden placed on both the interviewer and interviewee. There is a push in different fields of research to improve efficiency and to increase value for money; hence re-using existing data rather than generating new data is increasingly favored.However, the use of secondary data has a number of potential limitations and their implications that need to be noted and be mitigated for (Chauvette et al., 2019; Heaton, 2008; Hinds et al., 1997; Jacobson et al., 1993; Ruggiano & Perry, 2019; Sindin, 2017; Szabo & Strang, 1997). The key questions raised about the use of secondary qualitative data are related to data fitness, data quality, and limited clarity of the entire data collection procedure. These are in addition to ethical and legal implications of using secondary data (Chauvette et al., 2019).
(Sun & Lipsitz, 2018) in their article *Comparative effectiveness research methodology using secondary data: A starting user's guide* anticipated that research investigators would rely on secondary data to perform comparative effectiveness research better understand the necessity of a rigorous planning before study start and gain better insight in the choice of statistical methods so as to optimize the quality of the research study.

As indicated above this topic is geographical spread and I have insufficient resource, budget, or time for first-hand data collection to work around these limitations, I have used the method of using publicly available, online secondary data.

Data Analysis Plan

Step	Description
Objectives	Clearly outline the objectives of the data analysis plan, including identifying and mitigating fraud risks, ensuring sustainability, and adapting to the post-pandemic era.
Data Sources	Determine the relevant data sources, such as transactional data, customer data, employee data, and external data sources like industry reports or regulatory information.

Data Collection	Develop a data collection strategy, such as setting up automated data collection processes, integrating data from different systems, or conducting surveys or interviews to gather qualitative data.
Data Cleaning and Preparation	Clean and preprocess the collected data to ensure its quality and reliability, such as removing duplicates, handling missing values, standardizing data formats, and transforming data into a suitable format for analysis.
Fraud Risk Identification	Utilize data analysis techniques like statistical analysis, data mining, and machine learning algorithms to identify patterns and anomalies that may indicate potential fraud risks.
Fraud Risk Assessment	Assess the identified fraud risks based on their potential impact and likelihood of occurrence, such as assigning risk scores or probabilities to each identified risk.
Mitigation Strategies	Develop and implement appropriate fraud risk mitigation strategies based on the assessed risks, such as implementing fraud detection systems, enhancing internal controls, conducting employee training programs, or collaborating with external partners for fraud prevention.
Monitoring and Evaluation	Continuously monitor and evaluate the effectiveness of the implemented fraud risk management strategies, such as tracking key performance indicators (KPIs) related to fraud incidents, analyzing trends over time, and conducting periodic reviews or audits.
Reporting and Communication	Prepare comprehensive reports and communicate the findings and recommendations to relevant stakeholders, including senior management, board of directors, and employees.
Continuous Improvement	Regularly review and update the data analysis plan to incorporate new data sources, emerging fraud risks, and changes in the business environment.

Data Analysis

Data is a powerful tool that's available to organizations at a staggering scale. When harnessed correctly, it has the potential to drive decision-making, impact strategy formulation, and improve organizational performance. (Cote, 2021). Method Description: Content analysis involves systematically examining textual data, such as industry reports, corporate sustainability reports, financial disclosures, and regulatory documents. This method focuses on identifying recurring themes, trends, and patterns within the text. Application, I will conduct content analysis on relevant reports to uncover how organizations address fraud risk management and sustainability in their digital operations. This will involve categorizing and analysing language, key terms, and strategies used in reports to gain insights into their approaches.

Findings and Conclusion

The findings are that fraud risk management is important in the digital age and can be integrated into sustainable business practices. A framework for managing fraud risks in business needs to be provided, emphasizing the need for risk-based monitoring and evaluation of fraud risk management activities with a focus on outcome measurement. Some of the Leading practices for monitoring, evaluating, and adapting fraud risk management activities are provided. Further, the alternative approach to risk management in businesses is

proposed that takes into account the interrelationships between sources of risks and their potential impacts on business operations. The paper provides a theoretical model that relates risk management to sustainability. Overall, the research provides valuable insights into the integration of fraud risk management into sustainable digital business operations.
The importance of fraud risk management in the digital age and how it can be integrated into sustainable business practices. The paper provides a framework for managing fraud risks in systems and highlights the need for risk-based monitoring and evaluation of fraud risk management activities with a focus on outcome measurement. The paper also provides leading practices for monitoring, evaluating, and adapting fraud risk management activities. The paper proposes an alternative approach to risk management in businesses that considers the interrelationships between sources of risks and their potential impacts on business operations. The research provides a theoretical model that relates risk management to sustainability. Therefore, the conclusion is that incorporating fraud risk management into sustainable digital business operations is crucial for businesses to operate effectively and sustainably in the digital age.

Recommendations

Based on the findings in the information analysed I make the following recommendations that businesses should prioritize the integration of fraud risk management into their digital operations to ensure their sustainability in the post-pandemic era. They should adopt a comprehensive strategy that aligns fraud risk management cordially with sustainable business paradigms. Further, businesses should identify and classify the various types of fraud risks digital businesses are faced with in the post-pandemic era. With regards controls, businesses should implement robust internal controls to prevent fraud, including segregation of duties, regular audits, and monitoring of financial transactions. Employees are key in this, inevitably, businesses should train employees on fraud prevention to help in identifying fraudulent activities, reporting suspicious activities, and the consequences of fraudulent behaviour and should conduct background checks on their employees to ensure that they have no history of fraudulent activities.
To be agile, businesses should implement technology solutions such as fraud detection software, biometric authentication, and encryption to prevent fraud and should partner with reputable vendors to ensure that they are not involved in fraudulent activities and monitor financial statements regularly to detect any fraudulent activities. Businesses should encourage whistleblowing for employees to report any fraudulent activities without fear of retaliation.
By adopting these sustainable practices, businesses can prevent fraud and ensure business survival post-COVID-19.

References

Alkaabi, A. K. A. S., Adaikalam, J., Karim, A. M., Hock, O. Y., & Hossain, M. I. (2020). Influence on Internal Control through Digitalization of Assets: A Study on Ministry of Interior, UAE. International Journal of Academic Research in Accounting, Finance and Management Sciences, 10 (1): 13-24.

Alkaabi, A. K. A. S., Karim, A. M., Hossain, M. I., Nasiruzzaman, M. (2019). Assets Digitalization: Exploration of Prospects with Better Control Implementation. International Journal of Academic Research in Business and Social Sciences, 9(5), 960–970.

Alshams, Y. A. A. B, Hock, O. Y., Karim, A. M, Hossain, M. I. (2019). Developing a Framework on Performance and Challenges of Strategic Management Information System: A Case

study on Ministry of Interior, UAE. *International Journal of Academic Research in Business and Social Sciences*, 9(5), 633 – 646.

Alshamsi, H. S. A. A., Karim, A. M., Hossain, M. I. (2019) Effectiveness of Public Sector Financial Audit on Police Department of Abu Dhabi, UAE: Proposition of a Conceptual Framework. *International Journal of Academic Research in Business and Social Sciences*, 9(5), 647–659.

ACFE Insights(n.d.). *An Overview of the Federal Trade Commission's 2020 Consumer Reports*. https://www.acfeinsights.com/acfe-insights/overview-federal-trade-commission-2020-consumer-reports

Ariful, M., Mazuwin, Hossain, M. I. (2023). Innovation in a post-pandemic landscape: leveraging the power of strategic wisdom, International Journal of Management Concepts and Philosophy (IJMCP). https://doi.org/10.1504/IJMCP.2023.10055544

Association of Certified Fraud Examiners. (2022). ACFE Report to the Nations | 2022 Global Fraud Study. Www.acfe.com. https://legacy.acfe.com/report-to-the-nations/2022/

Awasthi, R., Guliani, K. K., Khan, S. A., Vashishtha, A., Gill, M. S., Bhatt, A., Nagori, A., Gupta, A., Kumaraguru, P., & Sethi, T. (2022). VacSIM: Learning effective strategies for COVID-19 vaccine distribution using reinforcement learning. Intelligence-Based Medicine, 6, 100060. https://doi.org/10.1016/j.ibmed.2022.100060

Botha, J. G., Botha, D., & Leenen, L. (2023). An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022. International Conference on Cyber Warfare and Security, 18(1), 36–48. https://doi.org/10.34190/iccws.18.1.1087

Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlstrom, P., & Henke, N. (2017). Artificial Intelligence The Next Digital Frontier? https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx

Cheong, H., Lyons, A., Houghton, R., & Majumdar, A. (2023). Secondary Qualitative Research Methodology Using Online Data within the Context of Social Sciences. International Journal of Qualitative Methods, 22, 160940692311801-160940692311801. https://doi.org/10.1177/16094069231180160

Choudhury, P. (2020). Our Work-from-Anywhere Future. Harvard Business Review. https://hbr.org/2020/11/our-work-from-anywhere-future

FTC. (2022). *Consumer Sentinel Network Data Book 2021*. Federal Trade Commission. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021

Cote, C. (2021). 4 Types of Data Analytics to Improve Decision-Making. Harvard Business School Online. https://online.hbs.edu/blog/post/types-of-data-analysis

WHO. (n.d.). Www.who.int. https://www.who.int/about/cyber-security

Davenport, T., & Kalakota, R. (2019). The potential for artificial intelligence in healthcare. *Future Healthcare Journal*, *6*(2), 94–98. ncbi. https://doi.org/10.7861/futurehosp.6-2-94

Nasdaq. (2022). Digital Transformation in a Post-Pandemic Era. Nasdaq.com. https://www.nasdaq.com/articles/digital-transformation-in-a-post-pandemic-era

Elkhwesky, Z., Salem, I. E., Varmus, M., & Ramkissoon, H. (2022). Sustainable practices in hospitality pre and amid COVID -19 pandemic: Looking back for moving forward post-COVID -19. Sustainable Development, 30(5). https://doi.org/10.1002/sd.2304

FBI. (2016). Health Care Fraud | Federal Bureau of Investigation. Federal Bureau of Investigation. https://www.fbi.gov/investigate/white-collar-crime/health-care-fraud

George, T. (2023). What is Secondary Research? | Definition, Types, & Examples. Scribbr. https://www.scribbr.com/methodology/secondary-research/

IMF (n.d.). How Pandemic Accelerated Digital Transformation in Advanced Economies. https://www.imf.org/en/Blogs/Articles/2023/03/21/how-pandemic-accelerated-digital-transformation-in-advanced-economies

FBI. (2016). *Health Care Fraud | Federal Bureau of Investigation*. Federal Bureau of Investigation. https://www.fbi.gov/investigate/white-collar-crime/health-care-fraud

Fontes, C., Hohma, E., Corrigan, C. C., & Lutge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. Technology in Society, 71, 102137. https://doi.org/10.1016/j.techsoc.2022.102137

ACFE (n.d.). *Fraud Risk Management Guide*. Www.acfe.com. Retrieved September 28, 2023, from https://acfe.com/fraud-resources/fraud-risk-tools---coso/fraud-risk-management-guide

Ghaffar Nia, N., Kaplanoglu, E., & Nasab, A. (2023). Evaluation of artificial intelligence techniques in disease diagnosis and prediction. Discover Artificial Intelligence, 3(1), 5. https://doi.org/10.1007/s44163-023-00049-5

Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. Sensors International, 2(2). https://doi.org/10.1016/j.sintl.2021.100117

Hossain, M. I., Alam, M. K., Johari, Z., Tasnim, M., Ferdaous, K. I., & Pal, T. (2023). Structural Modelling on Factors of Adopting FinTech Among Malaysian Millennials: Perceived COVID-19 Risk as Moderator. In *Digital Natives as a Disruptive Force in Asian Businesses and Societies* (pp. 134-156). IGI Global.

Hossain, M. I., Limon, N., Amin, M. T., & Asheq, A. S. (2018). Work Life Balance Trends: A Study on Malaysian GenerationY Bankers. *IOSR Journal of Business and Management,* 20 (9), 01-09.

Hossain, M. I., Maideen, M. B. H., Sharmin, N., & Islam, T. (2023). COVID-19 Repercussions on Bangladeshi On-Demand-Food Delivery, Restaurant, and Hotel Industry. *International Journal of Innovation and Business Strategy (IJIBS)*, *18*(1), 50-62.

Hossain, M. I., Maideen, M. B. H., Sharmin, N., & Islam, T. (2023). COVID-19 Repercussions on Bangladeshi On-Demand-Food Delivery, Restaurant, and Hotel Industry. *International Journal of Innovation and Business Strategy (IJIBS)*, *18*(1), 50-62.

Hossain, M. I., Ong, T. S., Tabash, M. I., & Teh, B. H. (2022). The panorama of corporate environmental sustainability and green values: evidence of Bangladesh. *Environment, Development and Sustainability*, 1-27.

Hossain, M. I., Ong, T. S., Tabash, M. I., Siow, M. L., & Said, R. M. (2022). Systematic literature review and future research directions: drivers of environmental sustainability practices in small and medium-sized enterprises. *International Journal of Sustainable Economy*, 14(3), 269-293.

Hossain, M. I., Polas, M. R. H., Rahman, M. M., Islam, T., & Jamadar, Y. (2020). An Exploration of COVID-19 Pandemic and its Consequences on FMCG Industry in Bangladesh. *Journal of Management Info*, 7(3), 145-155. https://doi.org/10.31580/jmi.v7i3.1484

Hossain, M. I., San, O. T., Ling, S. M., Said, R. M., & The, B. H. (2022). Nexus of Stakeholder Integration, Environmental Investment, Green Technology Adoption and Environmental Sustainability Practices: Evidence from Bangladesh Textile SMEs. *Journal of Social Sciences and Humanities*. 30 (1), 253 – 281. https://doi.org/10.47836/pjssh.30.1.14

Hossain, M. I., Teh, B. H., Tabash, M. I., Alam, M. N., & San Ong, T. (2022). Paradoxes on sustainable performance in Dhaka's enterprising community: a moderated-mediation

evidence from textile manufacturing SMEs. *Journal of Enterprising Communities: People and Places in the Global Economy*, (ahead-of-print).

Andersen, H. P. (2018). Sustainable Operations Management (SOM) Strategy and Management: An Introduction to Part I. *Operations Management and Sustainability*, 15–25. https://doi.org/10.1007/978-3-319-93212-5_2

Sanctionscanner (n.d). How Does AI-powered ID Verification Fight Digital Fraud? - Sanction Scanner. (n.d.). Sanctionscanner.com. https://sanctionscanner.com/blog/how-does-ai-powered-identity-verification-fight-digital-fraud-711

Jamadar, Y., Ong, T. S., Kamarudin, F., & Abdullah, A. A. (2022). Future firm performance, corporate governance, information asymmetry and insider trading–a systematic literature review using PRISMA. *International Journal of Sustainable Economy*, *14*(3), 309-329.

Jamadar, Y., San, O. T., Abdullah, A. A. and Kamarudin, F. (2021). Earnings and discretionary accruals. Managerial and Decision Economics. Doi: https://doi.org/10.1002/mde.3391

Javed, M., Hock, O. Y., & Asif, M. K., Hossain, M. I. (2020). Assessing the Impact of Emotional Intelligence on Job Satisfaction among Private School Teachers of Hyderabad, India. *International Journal of Psychosocial Rehabilitation.* 24(4). 5035-5045

Kshetri, N. (2015). Cybercrime and Cybersecurity Issues in the BRICS Economies. *Journal of Global Information Technology Management*, *18*(4), 245–249. https://doi.org/10.1080/1097198x.2015.1108093

Kumar, Y., Koul, A., Singla, R., & Ijaz, M. F. (2023). Artificial intelligence in disease diagnosis: a systematic literature review, synthesizing framework and future research agenda. Journal of ambient intelligence and humanized computing, 14(7), 8459–8486. https://doi.org/10.1007/s12652-021-03612-z

Kwekha-Rashid, A. S., Abduljabbar, H. N., & Alhayani, B. (2021). Coronavirus disease (COVID-19) cases analysis using machine-learning applications. *Applied Nanoscience*. https://doi.org/10.1007/s13204-021-01868-7

McAfee Labs COVID-19 Threats Report. (2020). https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/PDFs/McAfee/mcafee-072820-rp-quarterly-threats-july-2020.pdf

McKinsey & Company. (2020). COVID-19 digital transformation & technology | McKinsey. McKinsey & Company. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

Mughairi, B. M. A, Hajri, H. A., Karim, A. M., Hossain, M. I. (2019). An Innovative Cyber Security based Approach for National Infrastructure Resiliency for Sultanate of Oman. International Journal of Academic Research in Business and Social Sciences, 9(3) 1180–1195.

Nakamoto, S. (2008). Bitcoin: a Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

PwC (n.d.). *Navigating the rising tide of uncertainty PwC's 23rd Annual Global CEO Survey - Singapore Report*. Retrieved May 4, 2023, from https://www.pwc.com/sg/en/publications/assets/sg-ceo-survey-2020.pdf

Nur-Al-Ahad, M., Jamadar, Y., Latiff, A. R. A., Tabash, M. I., & Zaman, A. (2022, October). Effect of Islamic and Conventional Bonds on Firm's Performance: Evidence from Malaysia. In *2022 International Conference on Sustainable Islamic Business and Finance (SIBF)* (pp. 108-116). IEEE.

Ong, T. S., Teh, B. H., Sim, G. K., Ng, S. H., & Hossain, M. I. (2022). Does Dysfunctional Behavior Matter When it comes to Audit Quality in Malaysia?. *Asian Journal of Accounting and Governance*, 1-13.

Indeed. (n.d.). Operational Efficiency: Definition and Examples. Indeed Career Guide. https://www.indeed.com/career-advice/career-development/operational-efficiencies

Parker, K., Horowitz, J. M., & Minkin, R. (2022). COVID-19 Pandemic Continues To Reshape Work in America. Pew Research Center's Social & Demographic Trends Project; Pew Research Center. https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america/

APWG. (2020). Phishing E-mail Reports and Phishing Site Trends 4 Brand-Domain Pairs Measurement 5 Brands & Legitimate Entities Hijacked by E-mail Phishing Attacks 6 Use of Domain Names for Phishing 7-9 Phishing and Identity Theft in Brazil 10-11 Most Targeted Industry Sectors 12 APWG Phishing Trends Report Contributors 13 1st Quarter 2020 plus COVID-19 coverage Phishing Activity Trends Report Unifying the Glob a l Re sp onse T o Cyb er cr ime. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf?_gl=1

Powell, O. (2023). *A full timeline of the MGM Resorts cyber attack*. Cyber Security Hub. https://www.cshub.com/attacks/news/a-full-timeline-of-the-mgm-resorts-cyber-attack#:~:text=A%20timeline%20of%20the%20MGM

Prybylski, H. (n.d.). Two Years Into The Pandemic, Digital Transformation Is Moving Forward: Here's How. Forbes. Retrieved September 29, 2023, from https://www.forbes.com/sites/hankprybylski/2022/05/04/two-years-into-the-pandemic-digital-transformation-is-moving-forward-heres-how/?sh=a72c72a47739

Qureshi, R., Irfan, M., Gondal, T. M., Khan, S., Wu, J., Hadi, M. U., Heymach, J., Le, X., Yan, H., & Alam, T. (2023). AI in Drug Discovery and its Clinical Relevance. 9(7), e17575–e17575. https://doi.org/10.1016/j.heliyon.2023.e17575

Saleh, T. A., Sarwar, A., Khan, N., Tabash, M. I., & Hossain, M. I. (2023). Does emotional exhaustion influence turnover intention among early-career employees? A moderated-mediation study on Malaysian SMEs. *Cogent Business & Management*, *10*(3), 2242158.

Sarkis, J., Cohen, M. J., Dewick, P., & Schroder, P. (2020). A Brave New World: Lessons from the COVID-19 Pandemic for Transitioning to Sustainable Supply and Production. Resources, Conservation and Recycling, 159, 104894. https://doi.org/10.1016/j.resconrec.2020.104894

Sarkis, J., Cohen, M. J., Dewick, P., & Schroder, P. (2020). A Brave New World: Lessons from the COVID-19 Pandemic for Transitioning to Sustainable Supply and Production. Resources, Conservation and Recycling, 159, 104894. https://doi.org/10.1016/j.resconrec.2020.104894

Stackpole, B. (2021). Digital transformation after the pandemic. MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/digital-transformation-after-pandemic

State of Cyber Defense Report. (2023). Kroll. Retrieved September 29, 2023, from https://www.kroll.com/en/insights/publications/cyber/2023-state-cyber-defense#:~:text=Lack%20of%20trust%20ranked%20as

Takefuji, Y. (2023). Case report on enormous economic losses caused by fraud from Japan to the world. Journal of Economic Criminology, 1, 100003. https://doi.org/10.1016/j.jeconc.2023.100003

Fraud (2022). The History and Evolution of Fraud. Fraud.com. https://www.fraud.com/post/the-history-and-evolution-of-fraud

KPMG. (2022). *The supply chain fraud pandemic*. https://kpmg.com/xx/en/blogs/home/posts/2020/05/supply-chain-fraud-pandemic.html

Tovaglieri, F. (2021). How has the COVID-19 pandemic changed digital transformation? Hospitalityinsights.ehl.edu. https://hospitalityinsights.ehl.edu/what-next-digital-transformation

Uy, P. (2023). Enhancing Cybersecurity with Artificial Intelligence: A Game-Changer for the Digital Age. IPV Network. https://ipvnetwork.com/enhancing-cybersecurity-with-artificial-intelligence-a-game-changer-for-the-digital-age/

Wang, B., Liu, Y., Qian, J., & Parker, S. K. (2021). Achieving Effective Remote Working during the COVID-19 pandemic: a Work Design Perspective. Applied Psychology, 70(1), 16–59. Wiley.