ISSN No:-2456-2165

# The Disruptive Nature of Technology on the Business Environment: A Flipside to the Disruptive Beneifits

Darren S. Fisher
Faculty of BusinessAdministration,
LIGS University, Hawaii USA

**Abstract:- Businesses often ignore the disruptive nature of technology due to the over-reliance on the implied benefits versus concerns relating to utilization costs. However, the disruptive aspects of new and emerging technologies are worth exploring through academic research. There is no true success until businesses, and those impacted by digital transcendence understand the inherent challenges and risks of adopting new technologies to improve productivity, user experience, and potential financial gain. By exploring and understanding the deficiencies in the technological divide, companies can truly succeed in the digital transformation process by being appreciative of what challenges and risks to manage and mitigate. Going beyond the simple acknowledgment that knowledge transference will aid in fixing the learning gaps of technological change and grasp the need for governmental protective and supportive regulative policies to guide the digital ecosystem.**

***Keywords:-*** *Challenges, digital transformation, disruptive implications,emerging technologies, knowledge transfer, protection, regulation, risk.*

## I. INTRODUCTION

Organizations must capitalize on changes in the business environment and understand the implication of those changes, positive or negative. Through this approach, organizations can develop ambidextrous skills necessary to transcend the digital era and become success-driven entities. At this point, the pivotal moment of analysis, organizations can truly understand how these changes will add value and how they should manage challenges. True is similar in the case of new and emerging technologies; for too long focus has been on the positive impacts and not enough on the drawback. While technology claims to be the new paradigm creating a world filled with fast-paced communication and digital transactions, inversely is less desired from a business and regulatory standpoint.

Discourse in support of technology purports that existing, new, and emerging technologies provide conveniences that never existed before the digital age. Wellisz (2016) states in a report highlighting that the internet alone provides an avenue for scholars and academics to do more uncomplicated and less time-consuming research compared to physical libraries [21]. Secondly, academic literature insinuates that communication technology changes the way people perceive the world and the instances of commerce and banking. Wilburn and Wilburn (2018) also support that advancements in technologies such as artificial intelligence, the Internet of Things (IoT), and Big Data accelerate the capabilities of businesses to create value-added processes and product output decisions [22]. This enhancement in capabilities allows for increased creativity levels and customer delivery processes at lower prices [22]. With further progressions in emerging technologies such as autonomous vehicles, cryptography, and blockchain, the business environment continues to move in a direction once thought unimaginable.

In parallel studies by the author (2022) into government regulation and the implications on new and emerging technology, government, like business, has a specific role in the developmental cycle. On that premise, government regulatory frameworks become relevant in creating digital ecosystems conducive to developing and encouraging digital transformation. The study focuses primarily on the inherent benefits of digital technologies and the reasoning for adoption and gaps causing lag in developing countries. However, in the study of regulatory shielding (blocking) against new technologies, the author tests current ideologies driving the reasons behind such practices [8]. Coincidentally, the study cites that governments who engage in these blocking practices do it out of fear and unwillingness to accept the incomprehensive disruptive benefits of technology while fixated on the protection protocols against its drawbacks.

A critical review of literature on the topic provides insight into essential conceptual applications of digital technology and why governments in developing countries resist or adopt slower than more developed countries of similar or greater sizes. This report is essential to the body of research on government regulation and business innovation because it provides a holistic review of the paradigm from an inverse perspective. This perspective is valuable as academia focuses more on why governments

should support businesses in adopting new technologies but not why such technologies should be approached with caution and, in some cases, avoided.

Moreover, these peculiarities in academic literature give rise to the necessity to appreciate the negative implications of technology in greater detail and grasp the foundational issues associated with withdrawal symptoms in businesses and government. Additionally, further studies indicate that while technology has intrinsic value, the enthusiasm for technological change is often inherently biased and ill-perceived [11]. The resulting ideologies result from their analysis of different changes in the techno-economic systems, including those relating to incremental and radical innovations. However, current and prior research explain that challenges and risks temper the benefits of the digital age and, on that basis, gives credence to the need for pursuing a more in-depth analysis of the topic.

The essay examines the negative implications of digital technologies through theoretical impact assessment approaches. Firstly, digital technologies cause risks associated with their integration and use. There are points where the concepts of challenge and risk are considerably interchanged or broadly scoped as impacts, but by definition and theoretically, they are different—challenges or issues related to activities that occur as a result of an event. In contrast, risks or uncertainty is an event that can happen in the future. Afterwhich the essay will explore these perspectives from the lens of government regulation and why such frameworks appear valuable in blocking or providing strict policies against emerging and disruptive technologies. Lastly, the essay will conclude and give a conceptual review of existing findings and the implications for future research.

## II. THE NEGATIVE IMPLICATIONS OF EMERGING TECHNOLOGY

As explained in previous sections, the negative implications of new and emerging technologies are inconsequentially comparable to their ultimate disruptive benefits. In contrast, the application of technology projects exponential growth in performance units. Thus, making the exploration of the challenges and risks of these emerging technologies in the business's internal and external environment relevant. This essay seeks to provide unparallel clarity into understanding government action through policy designs and the building of sustainable holistic digital ecosystems that promote economic, transaction, and operational performance.

### *A. Challenges of Digital Technologies*

The discourse review provides a collative set of challenges businesses face when engaging in new and emerging technology. Figure 1 shows a graphical representation of the main challenges associated with such technologies proposed by [15]

*Information security challenges* speak to issues relating to the protection of business-sensitive data, including financial documentation, customer databases, or vital competitive information. These databases all inhibit vulnerabilities and digitalization processes. Another inherent challenge is businesses' default policies to manage information security, such as personal device policies that do not cater to business protection.


Fig. 1: Challenges of Emerging technology.
Source: Conceptual infographic designed by the author/researcher Fisher, D. S. (2022) to represent the challenges of emerging technologies by[18].

This challenge comes when the company does not have a corporate devise policy that can protect against potential data attacks. Romansky and Noninska (2020) identify that businesses must realize that information security is critical because it protects essential and valuable assets at different levels, whether computer, internet, communications, supplication, or network [19].

*Digital transformation*, in itself, is a challenge that organizations face, as the ultimate goal is not to integrate new technologies into every realm of a business. However, incidentally, digital transformation can be a biased and strenuous process that may lead to inconsistency with the user experience of the technology as such analysis and mindfulness are necessary when engaging in digitally transformative processes and the impact it has on the business and the user. Wilburn and Wilburn (2018) also cross-reference to other studies that integrating digital change is complex and must be done in tandem with balancing the impact on human capital [22].

*Compliance* is another challenge that organizations encounter after adopting new and emerging technology. Compliance requirements vary by organization, given industry, size, model, and consumers. However, this compliancy transcends organizational borders into the realm of legal requirements and industry standards. Hence understanding and identifying the relevant policy or regulations that govern compliance is often complex. A study by [3] in 2007 aligns with [18]in 2022 that organizations often face challenges developing policies given the regulatory requirements or lack thereof. As a result, some organizations create broad policies and do not cater to harmful details.

*Integration and upgrades* lead to similar issues with digital transformation, where management is critical. High costs and long periods are synonymous with these digital processes. Additionally, it includes deciphering complex communication requirements between new and existing systems and equipment. Businesses must detail communication networks and paths that make systems work effectively.

Like the previous challenges, *data management* impacts the business operation cycles, employees, and the requirement of constant access to information. Organizations face inherent challenges when integrating new technologies due to the difficulty in managing associated data. Concurrently, organizations struggle to identify role-based access to data and sometimes create hierarchical and bureaucratic delays in processes, and require extensive planning [18].

*Infrastructure changes* are another challenge businesses face when dealing with new and emerging technologies. According to [18], these changes impact an organization's Information Technology (IT) core systém structure. They often cause significant disruptions, translating into wastage of money and time as knowledge transfer between human capital occurs. Managing such infrastructure modifications and changes is equally very expensive and time absorptive. The opinions of this author also align with authors such as [22]. Additionally, they argue that discarding obsolete technology infrastructures is an added cost of change as part of the new technological change.

*Social media challenges* relate to the issue of creative distraction; this happens while at work and reduces productivity, especially in situations where employees work from home. Moreover, technology in its atmosphere can be very distracting in businesses, and as technology evolves, the levels of distraction grow. However, while social media is a relatively new challenge, it is relevant, and managing this can be expensive and require additional input like mobile management software. Like social media, focus on mobility is another significant new challenge due to the exponential growth of the mobile device market. The issue with this and emerging technologies is that as they evolve, so do the requirements for mobility and newer device. These rapid changes in pace may increase mobility costs. Concurrently, [18] states that this can make the enterprise mobile application experience challenging and less engaging.

Another linking challenge is the Internet of Things (IoT); while a relatively new technology in its own right, the challenge here is that IoT can be a critical pivot point if it is not a part of a digital transformation strategy. According to [18], organizations underestimate the impact and forget to map IoT in their infrastructure blueprint, thus creating avenues for security issues. On the other hand, automation often creates complications when integrated into workflows, and the transitional stages of new technologies také time and effort and often experience resistance [18]. Another recent challenge is those associated with the cloud. The cloud has come to a point where the market is full of possibilities, but not all solutions are equal. According to [18], the problem here is that adopting the incorrect resolution can be detrimental, and the corresponding management of the legacy systems becomes critical. While the cloud can be affordable, the quality can vary, and the challenge is ensuring the best fit for business needs which can be a frustrating process.

Remote work support has been increasing its popularity due to the advent of the Covid-19 pandemic, and with good reason. Perdomo (2022) argues in his article that new policies catering to work arrangements and remote technology access has been a challenge for companies using new technologies [18]. The author explains that organizations have to look at optimizing IT support services for remote work along with systém changes for troubleshooting and repairs.

While digital transformation and the adoption of emerging technology are essential to organizations, they can create a project management nightmare. Perdomo (2022) explains that the broad scope of digital transformation goals can cause a company to overspend, waste time, delay critical transformative initiatives and lead to instances of scope creep [18].

Another challenge of emerging technology is artificial intelligence (AI) issues. With many automation processes, this drives operation inclusive of Machine learning capabilities that allow for predictive processing AI technologies greatly disparity in quality. Thus choosing and

integrating the right technology is a challenge left for specialists. Perdomo (2022) argues that business processes are not always replicable and can cause AI functionality gaps [18].

A challenge that receives much discussion is the lack of technical training. Technical training is not critical but one of the foundational challenges why digital transformation processes fail. Accordingly, [18] explains that improving the technical capabilities of non-technical and operational staff is often met with grave resistance and reluctance. While technology aims to improve processes and productivity, effective training processes are also required.

*B. Risks of Digital Transformation*

The review of a broad cross-section of literature relating to the negative implications of digital transformation through the adoption of emerging technologies; businesses yields a diversity of risk factors. However, the author collates the ideologies across six risk categories (Fig. 2). As a precursor to the upcoming discussion, risks relate to those events that have not occurred.

As organizations venture into the digital arena, *cyber security risks* become a vital component of the—risk mitigation strategy. According to [21], cyber security risks are associated with the potential loss of personal or private digital data and require digital crimes relating to data. Subsequently, [21] insights that cyber security risks are numerous and difficult to quantify. As a result of cyber security risks comes cyber theft, cyberbullying, and many other cybercrimes. In their research, Romansky and Noninska (2020) highlight that cloud technologies and the internet of things open businesses to cyber security risks [19]. In their research, [19] indicate that seventy-six percent (76%) of business professionals believe that companies using IoT devices are susceptible to likely cyberattacks. Also, [17] alludes to the same concept where the article explains that cybersecurity is an outcome of the current digital world. On occasion, evidence in the news shares how large companies are continuously and increasingly under digital attack. In another study of the mining industry by [20], the authors explain that as digital transformation increase, so does cybersecurity risks. Notwithstanding, the authors allude to the broadened scope of digital transformation in its bid to connect different units within a business environment and, in turn, expose the entire business.

*Ethics and legality risk* is an all but too common ideology present in the literature on the topic. The majority of discourse explains that business ethics becomes a priority because anything that impacts stakeholder relations will lead to turmoil [14]. Throughout the research, [14] explain that technology tests norms and changes what people do or can do, act in response to people, and make decisions. Outside that general scope, technology has the potential to violate privacy and create financial and physical harm [14]. The author also argues that as technology evolves, so does the ability to embed values and political simulations that make decision-making simpler or complex, given the situation.

Concurrently, the authors also allude that technology can stereotype give essential characteristics such as race, gender, and age. Moreover, technological tools can abdicate responsibilities around decisions once executed by humans. These capabilities expose the adoption of new and emerging technologies to unforeseen ethical and legal complications in the daily operation of businesses.

*Performance and financial risks* are clear indicative risks of digital transformation. Too often, companies get caught up with being digital and forget what doing digital means—the misconception leads to excessive cost implications in the name of digital transformation. Referencing project management's challenge in earlier sections, companies incur scope creep, over-budget spending, loss of transformative focus, and delays due to lack of guidance. These issues relate to financial risks and can cause spiraling effects on a company's long-term performance [21] In some cases, these technology expenses can make or break a business if not managed; it includes infrastructure, training, specialist activities, policy alignments, and applicable technology fees. Notwithstanding the inherent risks associated with transformation itself are the financial risks related to cyber security breaches, which can bankrupt companies and stifle operations [19]

Subsequently, another critical category of adversity is knowledge and information risks. Discourse on the foundation of digital enhancement transference of knowledge and information comes to the forefront. As organizations transcend into the digital arena, knowledge is critical, and this process is often limited to the specialists that lead the process as technical knowledge is not easily transferrable. Additionally, the cost implications for prolonging training to get it right can negatively impact the businesses' bottom line. In contrast, information risks also pose additional issues regarding proprietary information and its ownership in a digital environment; new and emerging technologies often create grey areas for ownership and use.

*People risks* refers to the implications relating to human resources. While academics argue that technology and innovativeness improve workload, it also reduces the need for human capital. Technological restructuring can result in the loss of jobs and increase anxiety and

depression. Subsequently, [2] eloquently speak of the technostress side of technology. Their research defines technostress as the stressful experience of end-users in an organization due to their use of information, communication, and technology (ICT). As a result, they cite that technology can apply psychological and physiological costs to employees within an organization. Such demands result from increasing workloads, ergonomic stressors, role ambiguity, and monotonous tasks, which lead to organizational concerns [2]. These inherent risks find support in additional studies by [13] on the challenges of implementing technologies to manage health and safety in the construction environment. Although limited to a specific industry, the data is applicable across sectors where employees undergo a series of psychological factors considering new integrations.

The research also highlights other people's risks, such as work-life balance due to new technologies internal and external to the organization like social media. Employees can become guilty of distraction due to social media activities and other external technological advancements, impacting productivity in the Workplace. These are significant risk components that require careful analysis in an organization's bid to transform and encourage the integration of new technologies digitally. Beyond the personal impact on employees, risks also extend to employee fraud through technologies that provide access to consumers' data.

*Consumer and market risks* are those risks that can negatively impact the consumer or market environment that the business occupies. A limited source of literature explores the conditionalities that postulate the negative impacts of emerging technologies on the external business environment. However, literature shows that technology does impact the behavior of consumers and can, in turn, impact the way they relate to businesses. In an article by [1], the authors cite several risks manifest when dealing with new and emerging technologies in consumer markets. These include an operator or employee fraud and misconduct, platform vulnerability and unreliability, consumers disclosure in digital contexts, business model gap against consumer market needs, and the possibility of AI and machine learning creating biased decisions and outcomes for consumers. The primary issue is the business model misalignment from discourse, which leads to business failure and unmet market needs. Thus selecting the right technology and digital transformation strategy must align with market needs and expectations.

## III. REGULATING NEW TECHNOLOGIES

Throughout the in-depth analysis of the topic, evidence suggests that governments default to regulation and policy frameworks to protect themselves from the challenges and risks surrounding new and emerging technologies. Compared to studies by the author in 2022, this would appear a contradiction; however, wouldn't protection from the negative result in a better environment reap the disruptive benefits? Authors such as [9] support the author's view of regulation to support acceptance and make the environment conducive to technological advancements. Concurrently, [16] argues that government needs the right capabilities to develop solid regulative frameworks. Through these effectively drafted frameworks, consumers can get protection from the uncertainties of flexible and autonomous business models.

A Deloitte report by [5] states that new and emerging technologies risk national security through commercial use. The article highlights the need for government to regulate use but is hesitant because of the technologies applicability to military risks. The authors explain that as governments are willing to diffuse technologies, some are better limited to advancing military interests and not economic growth, such as certain drone technologies. There is much left to understand, but as governments seek to encourage digital adoption, they must ensure that they can manage the risks and challenges associated with emerging technologies and the processes that allow for true digital transformation.

## IV. CONCLUSION

In conclusion, evidence shows that new and emerging technologies exhibit disruptive implications on the business environment through many challenges and risks. While on the other hand, literature also explains why governments create policy frameworks to protect their actors while on the journey to transcend to a digital economy. Importantly, there is limited mix of academic research on the negative impacts of emerging technology, which leaves room for further analysis. This essay provides a base for further exploring the ideologies of managing challenges and mitigating risks associated with digital technologies in the business environment. Notwithstanding that academic articles give the necessary support on the benefits and why government regulation is needed, there are still gaps in understanding how detrimental new technology can be.

As technology evolves rapidly, so do the challenges and risks; hence, government regulations must be conducive, practical, and ethical. Government regulation and policy frameworks must strike that necessary balance to protect users of the technology while encouraging actors to

integrate and adopt digital advancements into their daily lives. It is only through a holistic understanding of the implications of emerging technologies can all stakeholders be willing, capable, and ready to maximize the disruptive benefits by managing and mitigating all underlying challenges and potential risk elements.

## REFERENCES

[1.] Boeddu, G., Chein, J., & Istuk, I. (2021, May 26). Addressing consumer risks in fintech to maximize its benefits. *World Bank Blogs*.

[2.] Bondanini, G., Giorgi, G., Ariza-Montes, A., Vega-Munoz, A., & Andreucci-Annziata, P. (2020, October 30). Technostress Dark Side of technology in the Workplace: a Scientometric Analysis. *International Journal of Environmental Research and Public Health*, 8013.

[3.] Debriabina, K., Ernest, A., & McAbee, B. (2007). Information Technology Regulatory Compliance and Information Security Management. *Journal of Comprehensive Research, 5*, 2.

[4.] Ebert, C., & Duarte, C. H. (2018). *Digital Transformation.* Retrieved November2021,fromResearchGate:https://www.researchgate.net/profile/CarlosHenriqueDuarte2/publication/326241618_Digital_Transformation/links/5b4d14f3aca27217ff9b05e4/Digital-Transformation.pdf

[5.] Ennis, H., Estevez, A., Meriani, J., Moran, J., & Pauloski, J. (2019, July 12). *Government Regulations for emerging technology*. Retrieved March 2022,fromDeloitteInsigths:https://www2.deloitte.com/us/en/insights/industry/public-sector/national-security-technology-regulation.html

[6.] Erik, S. (2008). Entrepreneurship and innovation policy. *Jena Economic Research Papers, 2008*(006).

[7.] Eunmi, L. (2020). Environmental Regulation and Financial Performance in China: An Integrated View of the Porter Hypothesis and Institutional Theory. *Sustainability, 12*(10183).

[8.] Fisher, D. S. (2022, March 17). Implications of Government Action on the Digital business economy | A Case Study on the Jamaican Economic and Innovative Environment. Retrieved March 2022, from LIGS University,Hawaii,USA:https://www.ligsuniversity.com/en/blogpost/implications-of-government-action-on-the-digital-business-economy-a-case-study-on-the-jamaican-economic-and-innovative-environment

[9.] Ganesh, Y. (2018, July 12). *Why we should be regulating technology instead of resisting it*. Retrieved March 2022, from Forbes: https://www.forbes.com/sites/forbescommunicationscouncil/2018/07/12/why-we-should-be-regulating-technology-instead-of-resisting-it/?sh=24b3a7df1032Hanna, N. (2018). A role for the state in the digital age. *Journal of Innovation and Entrepreneurship, 7*(5).

[10.] Kalthaus, M. (2020). Knowledge recombination along the technology life cycle. *Journal of Evolutionary Economics, 30*(ORCID: orcid.org/0000-0002-9177-3038), 643-704.

[11.] Kaplinksy, R., & Kraemer-Mbula, E. (2022). Innovation and uneven development: The challenge for low-and middle-income economies. *Research Policy, 51*(104394).

[12.] Luo, Y. (2021, April 4). A general framework of digitalization risks in international business. *Journal of International Business Studies.*

[13.] Malomane, R., Musonda, I., & Okoro, C. S. (2022). The Opportunities and Challenges Associated with the Implementation of Fourth Industrial Revolution technologies to Manage Health and Safety. *International Journal of Environmental Research and Public Health, 19*, 846.

[14.] Martin, K., Shilton, K., & Smith, J. (2019, June 19). Business and the Ethical Implications of Technology: Introduction to the symposium. *Journal of Business Ethics, 160*, 307-317.

[15.] Muriu, E. W. (2021). *The Impact of Digitalization on Internationalization of High-Tech Firms.* Lulea University of Technology, Department of Social Sciences, Technology and Arts.

[16.] Osimo, D. (2021, April 28). *New Technologies, New Markets: Why regulators must raise their game*. Retrieved March 2022, from The Lisbon Council: https://lisboncouncil.net/new-technologies-new-markets-why-regulators-must-raise-their-game/

[17.] Papiewski, J. (2019, March 19). *Huston Chronicle (Cron.).* Retrieved March 2022, from Technology's Negative Impact on Business: https://smallbusiness.chron.com/technologys-negative-impact-business-19118.htmlhttps://smallbusiness.chron.com/technologys-negative-impact-business-19118.html

[18.] Perdomo, R. (2022, January 1). *15 Technology challenges businesses may face in 2022*. Retrieved March 2022, from XsystemsX: https://blog.systems-x.com/technology-challenges-businesses-face

[19.] Romansky, R. P., & Noninska, I. S. (2020, August 10). *Challenges of the digital age for privacy and personal data protection*. *Mathematical Biosciences and Engineering.*

[20.] Sanchez, F., & Hartlieb, P. (2020, July 6). Innovation in the Mining Industry: Technological Trends and a Case Study of the Challenges of Disruptive Innovation.

*Mining, Metallurgy and Exploration, 37*, 1385-1399https://doi.org/10.1007/s42461-020-00262-1

[21.] Wellisz, C. (2016, September). The Dark Side of Technology. *Finance and Development*, *53*(3).

[22.] Wilburn, K. M., & Wilburn, H. R. (2018). T*he impact of technology on business and society*. *Global Journal of Business Research, 12*(1), 23-29.