Cybersecurity Risks and Threats in the Era of Pandemic-Induced Digital Transformation

(Authors Details)
Adeyemi Akinyemi
University of Houston, United States
Email: adey.akinyemi@gmail.com

Abstract

The phenomenal pace of digital transformation occasioned by the prevalent disruptions greatly transformed how organizations operated, communicated, and delivered services within industries. Although it has allowed organizations to remain operational and sustained, the introduction of remote work patterns, cloud computing, and online platforms also predisposed companies to increased cybersecurity threats and novel threats. The given paper explores the qualities and extent of the cybersecurity risks and threats, which facilitated during the pandemic-driven digital transformation, focusing on the increased attack surfaces, human-factor vulnerabilities, and the vulnerabilities in the digital infrastructure. The study is a synthesis of the available literature and reports on the industry to determine the common cyber threats like phishing, ransomware, malware propagation, and data breaches, as well as the systemic problems, including governance, policy implementation, and user awareness. Moreover, the research paper shows that these threats affect key sectors, such as healthcare, finance, education, and social institutions, in a disproportionate way. The studies highlight adaptive cybersecurity frameworks, sound risk management, and ongoing user education, which is the responsiveness of the research through the analysis of mitigation measures and best practices implemented during this time. The results can be used to better understand the restructuring of the cybersecurity environment under the actions of accelerated digital transformation and offer a point of view to build more resilient and secure cyber-ecosystems in future crises-related settings.

Keywords: Cybersecurity risks; Digital transformation; Pandemic-induced disruption; Cyber threats; Remote work; Information security; Risk management

DOI: 10.21590/ijtmh.07.4.06

Introduction

The unprecedented extent of disruption in the world caused by the prevalence of health crises increased the pace of digital transformation in economies, organizations, and societies. Physical interactions were limited, and digital technologies quickly became the main factors of economic continuity, remote work, digital trade, and collaboration across the borders. It was this sudden change that made the importance of cloud computing, online platforms, and data-driven systems

even more significant and reinvented the way value is generated, shared, and controlled within a digitally mediated economy (Ciuriak, 2020; Mak and Wang, 2016). Although digital transformation was a long-standing strategic goal of numerous organizations, the crisis situation condensed years of technological adoption into a much more limited time frame in which cybersecurity preparation often received inadequate consideration.

The expansion of remote and hybrid work models fundamentally altered organizational risk profiles. Employees increasingly accessed corporate systems from personal devices and unsecured home networks, weakening traditional perimeter-based security architectures (Kaufman et al., 2020). At the same time, labor market polarization driven by technology adoption exposed uneven access to digital skills and cybersecurity awareness, amplifying human-factor vulnerabilities (Park & Inocencio, 2020). These structural shifts created fertile ground for cybercriminal activities, as threat actors rapidly adapted their tactics to exploit uncertainty, fear, and operational weaknesses.

Beyond organizations, the digital transformation of economic and geopolitical interactions further complicated the cybersecurity landscape. Digital trade and data flows became central to post-crisis economic resilience, increasing exposure to cross-border cyber risks and regulatory fragmentation (Ciuriak, 2020; Bhowmick & Kamal, 2020). Simultaneously, rising techno-nationalism, misinformation, and narratives of techno-economic competition intensified concerns around cyber espionage and digital sovereignty (Siu & Chun, 2020; Soile & Balogun, 2020). Critical sectors such as finance faced compounded operational and cyber risks, as crisis management priorities often overshadowed long-term security investments (Vőneki, 2020).

These developments underscore the need to systematically examine cybersecurity risks and threats emerging from pandemic-induced digital transformation. Understanding how accelerated digital adoption, remote work practices, and evolving socio-political dynamics intersect with cybersecurity vulnerabilities is essential for building resilient digital ecosystems. This study therefore explores the nature of these risks and threats, situating cybersecurity not merely as a technical challenge but as a multidimensional issue shaped by economic, organizational, and human factors in a rapidly transforming digital era (Bangura et al.; ΜΠΑΚΑΛΗΣ, 2017).

Conceptual Framework

The accelerated adoption of digital technologies during pandemic-induced disruptions fundamentally reshaped organizational operations, economic activities, and social interactions. Digital transformation in this context refers to the integration of advanced digital tools, cloud-based solutions, and remote communication systems into organizational and societal processes to maintain continuity amid physical restrictions (Mak & Wang, 2016; Kaufman et al., 2020). While these transformations provided operational resilience, they also introduced complex cybersecurity vulnerabilities, particularly as organizations rapidly deployed remote work

infrastructures, cloud platforms, and digital service channels without comprehensive security protocols (Ciuriak, 2020; Park & Inocencio, 2020).

The conceptual framework of this study is anchored in the interplay between digital transformation drivers and cybersecurity risks. Key drivers include remote work adoption, digital trade expansion, telemedicine, e-learning, and virtual events, all of which accelerated during the pandemic (Kaufman et al., 2020; ΜΠΑΚΑΛΗΣ, 2017; Bhowmick & Kamal, 2020). These drivers expanded organizational attack surfaces, increasing susceptibility to threats such as phishing, ransomware, malware propagation, and data breaches. Simultaneously, socio-technical factors, including user awareness, organizational policies, and operational risk management, significantly modulated the extent of exposure (Vőneki, 2020; Siu & Chun, 2020).

The framework also incorporates sectoral implications, recognizing that industries such as finance, healthcare, education, and trade were disproportionately impacted due to their reliance on sensitive data and uninterrupted service delivery (Soile & Balogun, 2020; Bangura et al., 2020). In addition, geopolitical tensions and techno-economic competition intensified vulnerabilities, emphasizing the need for strategic cybersecurity governance (Siu & Chun, 2020; Ciuriak, 2020).

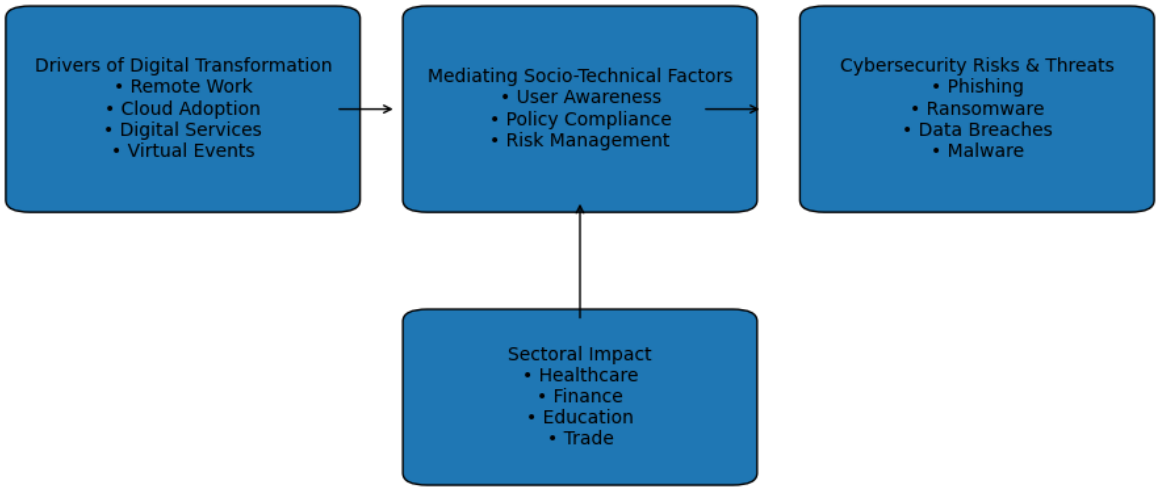

Fig 1: *This figure illustrates how pandemic-induced digital transformation drivers influence cybersecurity risks through socio-technical mediating factors, highlighting sector-specific vulnerabilities and opportunities for risk mitigation.*

Emerging Cybersecurity Risks

The rapid shift to digital platforms and remote operations during the pandemic-induced transformation introduced a range of cybersecurity risks across organizational and national contexts. Organizations faced new vulnerabilities as technology adoption accelerated without

corresponding security enhancements. Key emerging risks included expanded attack surfaces, human-factor vulnerabilities, insufficient infrastructure security, and threats arising from third-party dependencies (Ciuriak, 2020; Kaufman et al., 2020).

1. **Expanded Attack Surfaces**
   The widespread adoption of remote work and virtual collaboration tools increased the number of endpoints exposed to cyber threats. Organizations had to manage laptops, mobile devices, and home networks that often lacked enterprise-level security, creating multiple entry points for attackers (Kaufman et al., 2020; Park & Inocencio, 2020).

2. **Human-Factor Vulnerabilities**
   Social engineering attacks, including phishing and ransomware, capitalized on employee unfamiliarity with secure digital practices. Rapid onboarding, remote operations, and stress associated with pandemic conditions heightened the susceptibility of personnel to manipulation (Mak & Wang, 2016; Siu & Chun, 2020).

3. **Infrastructure and Third-Party Risks**
   The reliance on cloud services, SaaS platforms, and external vendors increased the complexity of maintaining robust cybersecurity. Weak security protocols in these third-party systems exposed organizations to data breaches and operational disruptions (Vőneki, 2020; Bhowmick & Kamal, 2020).

4. **Sector-Specific Vulnerabilities**
   Critical sectors, including healthcare, finance, and education, faced targeted attacks due to the high sensitivity of data and urgent operational demands during the crisis (Bangura et al., 2020; ΜΠΑΚΑΛΗΣ, 2017).

The table 1 below summarizes these emerging risks and their implications:

Emerging Cybersecurity Risk	**Description**	**Impact on Organizations**	**Reference**
Expanded attack surfaces	Remote work and digital tools increase potential entry points for attackers	Higher likelihood of unauthorized access and malware infiltration	Kaufman et al., 2020; Ciuriak, 2020
Human-factor vulnerabilities	Employees susceptible to phishing, ransomware, and social engineering	Compromise of sensitive data, operational disruption	Mak & Wang, 2016; Siu & Chun, 2020

Infrastructure and third-party risks	Dependence on cloud services and external vendors with weak security	Data breaches, service downtime, reputational damage	Vőneki, 2020; Bhowmick & Kamal, 2020
Sector-specific vulnerabilities	Targeted attacks on healthcare, finance, and education	Critical service disruption and economic loss	Bangura et al., 2020; ΜΠΑΚΑΛΗΣ, 2017

Overall, these risks highlight the urgent need for organizations to implement adaptive cybersecurity measures, strengthen employee awareness, and adopt resilient digital infrastructures capable of mitigating evolving threats in the era of pandemic-driven digital acceleration.

Major Cyber Threats Observed

The rapid shift to digital platforms and remote work models during the pandemic significantly altered the cybersecurity landscape, introducing a variety of threats that exploited both technological and human vulnerabilities. One of the most pervasive threats observed was phishing and social engineering attacks, which leveraged pandemic-related anxieties and misinformation to deceive users into divulging sensitive information (Ciuriak, 2020; Kaufman et al., 2020). Attackers frequently used COVID-19-themed emails, fake health advisories, and fraudulent communication from organizations to target employees working remotely.

Ransomware and malware attacks also surged, particularly in sectors experiencing accelerated digital adoption, such as healthcare, finance, and education (Vőneki, 2020; Park & Inocencio, 2020). These attacks disrupted critical operations and highlighted the vulnerability of networks that were rapidly expanded to accommodate remote access without robust security measures. Similarly, data breaches and unauthorized access incidents increased due to insecure endpoints, weak authentication, and the reliance on third-party cloud services (Mak & Wang, 2016; Bhowmick & Kamal, 2020).

In addition, cyber espionage and techno-economic threats emerged as significant concerns. Research indicated instances of state-sponsored and opportunistic attacks exploiting geopolitical tensions and the global shift to digital communication (Siu & Chun, 2020; Soile & Balogun, 2020). These threats included intellectual property theft, attacks on critical infrastructure, and targeted exploitation of digital trade networks (Ciuriak, 2020).

Risks associated with human behavior and organizational policies were exacerbated by remote work arrangements, where employees frequently bypassed security protocols for convenience or lacked sufficient cybersecurity awareness (Kaufman et al., 2020; ΜΠΑΚΑΛΗΣ, 2017; Bangura,

Obi, & Mngutyo, 2020). The combination of technical vulnerabilities and human factors created a complex threat environment, underscoring the need for comprehensive risk management and adaptive security strategies.

Organizational and Human Factors

The pandemic-induced shift toward remote work and accelerated digital transformation significantly altered the organizational and human dimensions of cybersecurity. Organizations were compelled to adopt digital platforms and virtual collaboration tools rapidly, often without fully integrated security protocols. This sudden digital transition expanded the attack surface, leaving critical systems more vulnerable to cyber threats (Ciuriak, 2020; Mak & Wang, 2016). Financial institutions, healthcare providers, and educational organizations, in particular, faced heightened operational risks due to inadequate crisis management and insufficiently tested security infrastructures (Vőneki, 2020).

Human factors played a crucial role in exacerbating cybersecurity vulnerabilities. Employees working from home often relied on personal devices and unsecured networks, increasing susceptibility to phishing attacks, malware, and social engineering exploits (Kaufman et al., 2020). Furthermore, varying levels of digital literacy and insufficient cybersecurity training hindered effective risk mitigation, amplifying the potential for human error (Park & Inocencio, 2020). Cultural and socio-political dynamics also influenced organizational responses, with biases and misinformation shaping decision-making processes and cross-border collaborations (Siu & Chun, 2020; Soile & Balogun, 2020).

Resource constraints and competing organizational priorities further complicated the cybersecurity landscape. Companies frequently faced trade-offs between operational continuity and security investments, particularly in emerging markets and sectors undergoing rapid digitalization (Bhowmick & Kamal, 2020; Bangura, Obi, & Mngutyo, 2020). Additionally, sectors such as real estate and hospitality experienced structural disruptions that intensified pressure on staff and management, contributing to gaps in protocol enforcement and awareness (ΜΠΑΚΑΛΗΣ, 2017).

Overall, the interplay of organizational preparedness, human behavior, and socio-economic factors shaped the cybersecurity risks during the pandemic, highlighting the need for integrated strategies that combine technology, policy, and workforce training to strengthen resilience against evolving cyber threats.

Impact on Critical Sectors

The rapid digital transformation triggered by pandemic-induced disruptions had profound effects across critical sectors. While technology adoption enabled operational continuity, it also exposed

organizations to elevated cybersecurity risks and operational vulnerabilities. The following analysis highlights the sector-specific impacts:

1. Healthcare Sector

Healthcare institutions rapidly shifted to digital platforms for telemedicine, electronic health records, and patient management. This transformation increased exposure to ransomware attacks, phishing campaigns targeting healthcare staff, and data breaches compromising sensitive patient information (Ciuriak, 2020). Limited cybersecurity preparedness amplified operational risks during crisis periods.

2. Financial Sector

The financial sector experienced heightened operational and cybersecurity risks due to increased online transactions, remote banking operations, and cloud dependency. Cyberattacks on banking systems, including phishing and malware, became more prevalent, affecting transaction security and customer trust. Crisis and operational risk management strategies were critical to mitigating these impacts (Vőneki, 2020).

3. Education Sector

Schools and universities transitioned to online learning platforms, often without adequate cybersecurity frameworks. This shift exposed educational institutions to data breaches, unauthorized access to learning management systems, and digital fraud targeting students and staff (Park & Inocencio, 2020).

4. Corporate Sector (Remote Work and MICE Industry)

Remote work proliferation increased dependence on virtual collaboration tools, raising endpoint security vulnerabilities (Kaufman et al., 2020). The Meetings, Incentives, Conferences, and Exhibitions (MICE) industry also faced challenges in digital adoption, requiring secure platforms for virtual events (Mak & Wang, 2016).

5. Public Sector and International Cooperation

Government agencies and international organizations relied on digital platforms for communication and diplomacy, increasing exposure to cyber espionage and ransomware attacks (Soile & Balogun, 2020; Siu & Chun, 2020). Weak digital governance in some regions intensified these risks, threatening continuity in public service delivery.

6. Real Estate and Infrastructure

Teleworking influenced commercial real estate usage, increasing reliance on digital access systems and smart building technologies. Insufficient cybersecurity protocols in smart infrastructure heightened the risk of unauthorized access and operational disruptions (ΜΠΑΚΑΛΗΣ, 2017).

Table 2: Sectoral Impact Summary Table

Sector	Key Digital Transformation	Major Cybersecurity Risks	Operational Impacts	References
Healthcare	Telemedicine, EHRs	Ransomware, phishing, data breaches	Service disruption, patient data compromise	Ciuriak, 2020
Financial	Online banking, Cloud	Malware, phishing, cyber fraud	Transaction risks, reduced trust	Vőneki, 2020
Education	Online learning platforms	Unauthorized access, data theft	Disrupted learning, compromised student data	Park & Inocencio, 2020
Corporate / MICE	Remote work, Virtual events	Endpoint vulnerabilities, phishing	Productivity loss, operational inefficiency	Kaufman et al., 2020; Mak & Wang, 2016
Public / Government	E-governance, Digital diplomacy	Cyber espionage, ransomware	Policy delays, public trust issues	Soile & Balogun, 2020; Siu & Chun, 2020
Real Estate / Infrastructure	Teleworking, Smart buildings	Unauthorized access, system breaches	Operational disruption, security risks	ΜΠΑΚΑΛΗΣ, 2017

The table highlights that while digital transformation provided essential continuity during pandemic disruptions, it also created sector-specific cybersecurity vulnerabilities. Understanding these impacts is crucial for developing targeted mitigation strategies and resilient digital infrastructures across critical sectors.

Mitigation Strategies and Best Practices

The pandemic-induced acceleration of digital transformation amplified the exposure of organizations to cybersecurity threats. To address these challenges, a combination of technological, organizational, and human-centric mitigation strategies emerged as best practices.

1. Strengthening Cybersecurity Governance and Risk Management

Organizations emphasized the importance of establishing robust governance frameworks that integrate cybersecurity into overall risk management processes. Clear policies, accountability structures, and continuous monitoring were identified as critical components for managing operational and digital risks (Vőneki, 2020). Crisis management frameworks were adapted to include cyber risk assessments, scenario planning, and rapid response mechanisms, ensuring resilience against both anticipated and unforeseen cyber incidents.

2. Adoption of Secure Digital Infrastructures

The transition to remote work and cloud-based platforms highlighted vulnerabilities in endpoints, networks, and data storage systems. Best practices included the implementation of multi-factor authentication (MFA), encryption of sensitive data, secure virtual private networks (VPNs), and regular software updates to mitigate potential breaches (Kaufman et al., 2020). Cloud service providers and third-party vendors were carefully vetted to ensure compliance with organizational security standards (Ciuriak, 2020).

3. Zero-Trust and Access Management Models

Organizations increasingly adopted zero-trust security models, emphasizing "never trust, always verify" principles. This approach limits access privileges based on user roles, continuous monitoring of user activities, and verification of device and application integrity, reducing potential attack surfaces (Mak & Wang, 2016).

4. Employee Awareness and Training Programs

Human factors remained a significant source of vulnerability, particularly with the rise of phishing and social engineering attacks. Regular cybersecurity awareness campaigns, simulated phishing exercises, and training on safe digital practices were widely implemented to cultivate a security-conscious workforce (Park & Inocencio, 2020; Siu & Chun, 2020). Organizations recognized that technology alone cannot counter threats without informed users.

5. Sector-Specific and Collaborative Strategies

Critical sectors such as healthcare, finance, and education implemented tailored mitigation measures. In the financial sector, operational risk management was enhanced to include continuous monitoring and regulatory compliance (Vőneki, 2020). Cross-border cooperation, information sharing, and joint cybersecurity initiatives also emerged as effective strategies,

especially in regions experiencing interconnected pandemic-induced economic disruptions (Bhowmick & Kamal, 2020; Soile & Balogun, 2020).

6. Continuous Monitoring and Incident Response

The implementation of real-time threat detection systems, security information and event management (SIEM) tools, and automated alert mechanisms enabled organizations to identify and respond to breaches promptly. Rapid incident response and post-incident analysis strengthened organizational resilience and informed future mitigation strategies (Bangura, Obi, & Mngutyo, 2020; ΜΠΑΚΑΛΗΣ, 2017).

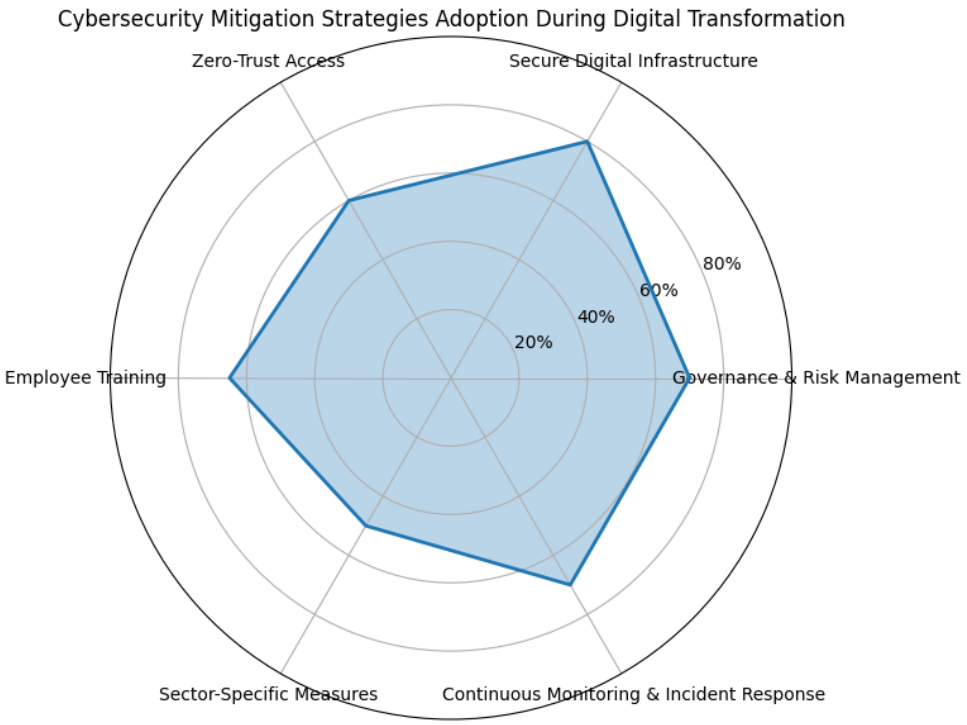

Fig 2: The radar chart shows estimated adoption levels of key cybersecurity mitigation strategies during pandemic driven digital transformation, expressed as percentages across governance, infrastructure, access control, training, sector specific controls, and continuous monitoring.

Effective mitigation during this period required a multi-layered approach integrating technological safeguards, human-factor considerations, governance enhancements, and collaborative efforts. By adopting these strategies, organizations were able to reduce exposure to cyber threats and maintain operational continuity amidst unprecedented digital acceleration (Ciuriak, 2020; Kaufman et al., 2020; Vőneki, 2020). These best practices provide a foundation for ongoing resilience as organizations continue to navigate increasingly complex digital environments.

Conclusion and Future Research Directions

The rapid digitalization caused by the disruption of pandemic conditions seriously changed the working and technological environment in the organizations of the world. This study shows that the continuity was made possible by the digital adoption, including remote work, cloud computing, and delivering services digitally but also brought a wide range of cybersecurity risks and threats. The major vulnerabilities were increased attack areas, human factors vulnerabilities, inadequate security measures, and use of third party and cloud systems (Kaufman et al., 2020; Mak and Wang, 2016). Healthcare, finance, and education are key sectors that were overrepresented in the list of impacted ones, with consequences of operations, economics, and reputation (Vőneki, 2020; Park and Inocencio, 2020). Moreover, the overlap of cybersecurity threats and socio-political tensions, including techno-orientalism and cyber espionage, make it clear that the modern cyber risk environment is a complex phenomenon (Siu and Chun, 2020).
The mitigation measures that were implemented at this time, such as the use of adaptive cybersecurity systems, risk treatment procedures, and user education efforts, played a critical role in minimizing exposure and promoting resilience (Ciuriak, 2020; Bhowmick and Kamal, 2020). However, systematic gaps in policies, policies implementation, and transnational cooperation in the digital sector signify that the systemic interventions become more robust (Soile & Balogun, 2020; Bangura et al., 2020).

Future Research Directions

Future research is to be carried out to create dynamic cybersecurity models responsible for the ongoing development of threats within the crisis-inflicted digital landscape. The studies of the implementation of artificial intelligence and automated threat detection solutions in the remote and hybrid work systems can be used to improve organizational resilience further. Also, the comparative analyses of sector-specific cybersecurity vulnerabilities and mitigation measures will be useful in offering actionable information to policy makers and industry leaders. International collaboration and harmonization of digital policies will also become essential in the context of dealing with the new global cyber threats through cross-national research (Bhowmick and Kamal, 2020; ΜΠΑΚΑΛΗΣ, 2017). Finally, exploring the socio-technical and human behavioral aspects of cybersecurity in digitally accelerated settings can provide comprehensive measures of fortifying organizational defenses in future disruptive settings.

References

1. Ciuriak, D. (2020). Digital Trade in a Post-Pandemic Data-Driven Economy. *Available at SSRN 3617251*.
2. Mak, C., & Wang, P. K. (2016). Digital transformation in Singapore's MICE industry.

3. Kaufman, E., Lovich, D., Bailey, A., Messenböck, R., Schuler, F., & Shroff, A. (2020). Remote work works–where do we go from Here. *BCG. URL*.
4. Park, C. Y., & Inocencio, A. M. (2020). COVID-19, technology, and polarizing jobs.
5. Siu, L., & Chun, C. (2020). Yellow peril and techno-orientalism in the time of Covid-19: racialized contagion, scientific espionage, and techno-economic warfare. *Journal of Asian American Studies*, *23*(3), 421-440.
6. Vőneki, Z. (2020). Crisis management and operational risk management in the financial sector in the shadow of COVID-19. *Economy & finance*.
7. Bhowmick, S., & Kamal, S. M. (2020). India-Bangladesh Partnership in Post-Pandemic Economic Recovery. *Observer Research Foundation (ORF) special report*, *119*.
8. Soile, O., & Balogun, W. A. (2020). 'Pandemic Diplomacy'and the Politics of Paradox: International Cooperation in the Age of National Distancing. *Gaziantep Üniversitesi Sosyal Bilimler Dergisi*, *19*(COVID-19 Special Issue), 413-428.
9. Bangura, I., Obi, C., & Mngutyo, I. D. Conclusion: Shifting from Business as Usual–Youth and the Future of Africa. In *African Youth during the COVID-19 Pandemic* (pp. 152-169). Routledge.
10. Amuda, B. (2020). Integration of Remote Sensing and GIS for Early Warning Systems of Malaria Epidemics in Nigeria. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *12*(02), 145-152.
11. Bello, I. O. (2020). The Economics of Trust: Why Institutional Confidence Is the New Currency of Governance. *International Journal of Technology, Management and Humanities*, *6*(03-04), 74-92.
12. Bodunwa, O. K., & Makinde, J. O. (2020). Application of Critical Path Method (CPM) and Project Evaluation Review Techniques (PERT) in Project Planning and Scheduling. *J. Math. Stat. Sci*, *6*, 1-8.
13. Isqeel Adesegun, O., Akinpeloye, O. J., & Dada, L. A. (2020). Probability Distribution Fitting to Maternal Mortality Rates in Nigeria. Asian Journal of Mathematical Sciences.
14. Bello, I. O. (2021). Humanizing Automation: Lessons from Amazon's Workforce Transition to Robotics. *International Journal of Technology, Management and Humanities*, *7*(04), 41-50.
15. ΜΠΑΚΑΛΗΣ, Α. (2017). The impact of the COVID-19 pandemic and the subsequent rise of teleworking on the real estate sector in Greece.