# Intrusion Detection and Prevention Models for Enhancing Organizational Cyber Defense Effectiveness

ADETOMIWA A. DOSUNMU[1], PETER OLUSOJI OGUNDELE[2]
[1]*Adbirt Nigeria, Lagos, Nigeria*
[2]*Ericsson, Lagos Nigeria*

***Abstract- The increasing dependence of organizations on digital infrastructure has amplified exposure to cyber threats that are sophisticated, persistent, and highly adaptive. Traditional perimeter-based security mechanisms have proven insufficient in detecting and mitigating advanced attacks that exploit system vulnerabilities, insider access, and zero-day exploits. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have therefore become central components of organizational cyber defense strategies. Over the last two decades, research has produced a wide range of intrusion detection and prevention models, spanning signature-based, anomaly-based, specification-based, and hybrid approaches, as well as centralized, distributed, and collaborative architectures. This paper reviews and synthesizes research on IDS and IPS models published, with the aim of evaluating their effectiveness in enhancing organizational cyber defense. The study examines detection techniques, architectural designs, deployment strategies, performance metrics, and organizational integration challenges. By consolidating existing knowledge, the paper highlights key strengths and limitations of prevailing models and provides a conceptual basis for understanding how intrusion detection and prevention mechanisms contribute to proactive, resilient, and adaptive cyber defense in organizational contexts.***

***Keywords- Intrusion detection systems; Intrusion prevention systems; Cyber defense; Network security; Anomaly detection; Organizational security***

## I. INTRODUCTION

Organizations across all sectors increasingly rely on interconnected information systems to support core operations, decision making, communication, and service delivery [1], [2], [3]. This dependence has significantly expanded the attack surface available to malicious actors, exposing organizations to a wide range of cyber threats including malware, denial-of-service attacks, unauthorized access, data exfiltration, and insider misuse [4], [5]. Cyber incidents can disrupt operations, compromise sensitive information, damage organizational reputation, and result in substantial financial losses [6], [7]. As a result, cyber defense has become a strategic priority for organizations, requiring layered, adaptive, and intelligence-driven security mechanisms.

Early approaches to organizational cybersecurity focused primarily on perimeter defenses such as firewalls, access control mechanisms, and authentication systems. While these controls remain essential, they are largely preventive in nature and assume that threats originate outside organizational boundaries [8], [9]. Over time, it became evident that such assumptions are insufficient, particularly in environments characterized by mobile computing, cloud services, remote access, and complex supply chains [10], [11]. Attackers increasingly bypass perimeter defenses through social engineering, credential theft, misconfigurations, and exploitation of trusted relationships. Consequently, organizations require security mechanisms capable of monitoring system behavior, detecting malicious activity in real time, and responding to intrusions that evade preventive controls [12], [13].

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) emerged as critical components of this defensive posture. IDS are designed to monitor network traffic or host activities to identify patterns indicative of malicious behavior, while IPS extend this capability by actively blocking or mitigating detected threats. Together, IDS and IPS support the transition from static security models toward dynamic and responsive cyber defense architectures [14], [15]. Their role is particularly important in organizational settings where systems are heterogeneous, users exhibit diverse behaviors, and threats evolve rapidly.

The conceptual foundations of intrusion detection were established through the recognition that malicious activity often manifests as deviations from normal system behavior or as identifiable patterns associated with known attacks [16], [17]. Early research distinguished between misuse detection, which relies on signatures of known attacks, and anomaly detection, which models normal behavior and flags deviations as potential intrusions [18], [19]. Each approach offers distinct advantages and limitations. Signature-based systems provide high accuracy for known threats but struggle with novel or obfuscated attacks. Anomaly-based systems offer greater potential for detecting previously unseen attacks but are prone to false positives, which can overwhelm security teams and reduce trust in detection mechanisms [20], [21].

As organizational networks grew in scale and complexity, intrusion detection models evolved to address new challenges. Distributed IDS architectures were proposed to monitor activity across multiple network segments, while host-based systems focused on detecting attacks that bypass network-level monitoring [22], [23]. Hybrid systems combined network-based and host-based detection to improve coverage and accuracy [24], [25]. Research also explored specification-based detection, which defines expected system behavior through formal rules and detects violations of those specifications. These developments reflected an ongoing effort to balance detection accuracy, computational efficiency, scalability, and operational practicality [26], [27].

Intrusion prevention introduced additional complexities. While detection focuses on identifying malicious activity, prevention requires timely and reliable decision making to block attacks without disrupting legitimate operations [28]. In organizational environments, overly aggressive prevention mechanisms can lead to service degradation, loss of availability, or unintended denial of legitimate access. As a result, IPS design must carefully consider response strategies, confidence thresholds, and integration with broader security management processes [29], [30]. Research examined various prevention models, including inline network devices, host-based enforcement mechanisms, and policy-driven response systems that incorporate human oversight [31].

The effectiveness of IDS and IPS models cannot be assessed solely in technical terms. Organizational factors such as security policies, governance structures, incident response capabilities, user awareness, and resource constraints play a critical role in determining how these systems contribute to overall cyber defense [32], [33]. Many studies have noted that technically sophisticated detection models may fail to deliver value if they generate excessive false alarms, lack interpretability, or are poorly integrated into organizational workflows. Conversely, simpler models that align well with organizational processes may provide more practical benefits despite lower theoretical detection performance [34].

Another key driver of research has been the increasing availability of data and computational resources [35], [36]. Machine learning and data mining techniques gained prominence in intrusion detection research, offering tools for modeling complex patterns in network traffic and system behavior. Techniques such as decision trees, support vector machines, neural networks, clustering algorithms, and ensemble methods were widely explored [37], [38]. These approaches promised improved detection accuracy and adaptability but also introduced challenges related to training data quality, model interpretability, and computational overhead. In organizational settings, concerns about explainability and trust further influenced the adoption of learning-based IDS and IPS models [39], [40].

The growing prevalence of advanced persistent threats underscored the need for detection models capable of identifying low-and-slow attacks that evade traditional signatures [41], [42]. Such threats often involve multi-stage campaigns, lateral movement, and prolonged reconnaissance, making them difficult to detect through isolated events. Research therefore increasingly emphasized correlation, context awareness, and behavioral analysis across time and system layers [43], [44]. Collaborative and cooperative IDS models were proposed to share information across organizational boundaries or security domains, enhancing situational awareness and early warning capabilities [45].

Despite extensive research, organizations continue to face challenges in deploying and operating effective IDS and IPS solutions. Issues such as high false-positive rates, limited visibility into encrypted traffic, performance overhead, and the shortage of skilled security professionals persist [46], [47]. Furthermore, the rapid evolution of attack techniques means that detection and prevention models must continuously adapt to remain effective. These challenges highlight the importance of synthesizing existing research to understand which models are most suitable for different organizational contexts and how they can be combined into cohesive cyber defense strategies [48], [49].

The objective of this paper is to review and synthesize intrusion detection and prevention models developed, with a focus on their role in enhancing organizational cyber defense effectiveness. The paper examines detection paradigms, architectural designs, analytical techniques, and deployment considerations, drawing on a broad body of literature. By consolidating insights across these dimensions, the study aims to clarify the strengths and limitations of prevailing approaches and to provide a structured understanding of how IDS and IPS contribute to organizational security resilience.

The remainder of this paper is organized as follows. Section 2 presents a comprehensive literature review of intrusion detection and prevention models, including detection techniques, system architectures, machine learning applications, and organizational considerations. Subsequent sections synthesize these findings and discuss implications for practice and research.

## II. LITERATURE REVIEW

Research on intrusion detection and prevention has evolved significantly as cyber threats have grown in sophistication and scale. Early studies focused on defining the problem of intrusion detection and establishing foundational detection paradigms [3], [7]. The seminal distinction between misuse detection and anomaly detection shaped much of the subsequent research [10]. Misuse detection systems rely on predefined signatures that describe known attack patterns. These systems are effective at identifying previously observed threats with high precision, making them attractive for operational deployment. However, their dependence on signature databases limits their ability to detect novel or polymorphic attacks, a weakness repeatedly documented in the literature [50], [51].

Anomaly detection approaches were introduced to address these limitations by modeling normal system or network behavior and flagging deviations as potential intrusions. Techniques for anomaly detection include statistical profiling, time-series analysis, clustering, and machine learning [52], [53]. Early anomaly-based IDS demonstrated the feasibility of detecting unknown attacks but also revealed significant challenges related to false positives and model drift. In organizational environments, where legitimate behavior can vary widely across users and applications, defining "normal" behavior is inherently complex [54], [55].

Specification-based detection represents an intermediate approach, combining aspects of misuse and anomaly detection. In this paradigm, expected system behavior is defined through formal specifications, and deviations from these specifications are treated as intrusions. Specification-based IDS aim to reduce false positives while retaining the ability to detect previously unknown attacks. Studies have shown that this approach is particularly effective in well-defined application domains, though it requires significant effort to develop and maintain accurate specifications [56], [57].

Architectural considerations have also played a central role in IDS and IPS research. Network-based IDS monitor traffic at strategic points within the network, providing visibility into communication patterns and potential attacks targeting multiple hosts. Host-based IDS focus on activities within individual systems, such as file access, process execution, and system calls. Hybrid architectures combine both approaches to improve coverage and accuracy. Distributed IDS architectures were proposed to address scalability and fault tolerance, enabling detection across large, heterogeneous organizational networks [58], [59].

Intrusion prevention extended detection research by emphasizing automated response. IPS models can be implemented inline within network traffic paths or at host level, where they intercept malicious activity and enforce security policies. Research explored various response strategies, including packet dropping, connection termination, access control updates, and alert escalation. A recurring theme in the literature is the trade-off between responsiveness and reliability, as false positives in prevention systems can have severe operational consequences [60], [61].

The application of machine learning techniques became increasingly prominent in IDS research. Supervised learning methods such as decision trees, k-nearest neighbors, support vector machines, and neural networks were widely studied for classifying network traffic or system events as benign or malicious. Unsupervised learning techniques, including clustering and self-organizing maps, were applied to anomaly detection in environments where labeled data were scarce [62], [63]. Ensemble methods and hybrid models sought to combine multiple classifiers to improve detection accuracy and robustness [64].

While learning-based models demonstrated promising results in experimental settings, their deployment in organizational environments raised practical concerns [65], [66]. Training data quality, class imbalance, evolving attack patterns, and the lack of interpretability were frequently cited challenges. Security analysts often require explanations for alerts to support incident response and forensic analysis, yet many machine learning models function as black boxes. Research therefore explored feature selection, model simplification, and rule extraction techniques to enhance interpretability and usability [67].

Another important line of research examined IDS performance metrics and evaluation methodologies. Common metrics include detection rate, false-positive rate, accuracy, precision, recall, and response time. However, studies emphasized that these metrics must be interpreted in the context of organizational goals and constraints. For example, a system with high detection accuracy but excessive false alarms may be impractical for organizations with limited security staff. Test datasets, such as benchmark intrusion detection datasets, were widely used for evaluation, though their representativeness of real-world traffic was often questioned [68], [69].

The emergence of advanced persistent threats prompted research into multi-stage and behavior-based detection models [70], [71]. These approaches focus on correlating events over time, across hosts, and across network layers to identify coordinated attack campaigns. Techniques such as attack graphs, Bayesian inference, and temporal correlation were employed to capture the progression of complex intrusions. Such models align closely with organizational needs, as they support strategic threat hunting and long-term risk assessment [72], [73].

Collaborative and cooperative intrusion detection models were also explored, particularly in contexts where information sharing could enhance situational awareness. By aggregating alerts and threat intelligence from multiple sources, collaborative IDS aim to detect widespread or emerging attacks more effectively. Research examined trust models, data sharing protocols, and privacy considerations associated with such collaboration, recognizing both its potential benefits and organizational challenges [74].

From an organizational perspective, the literature consistently emphasizes that IDS and IPS effectiveness depends on integration with broader security management processes. Detection and prevention systems must align with incident response plans, security policies, compliance requirements, and risk management frameworks. Studies have highlighted the importance of human factors, including analyst expertise, alert fatigue, and organizational culture, in shaping the real-world impact of IDS and IPS deployments [75], [76].

Performance and scalability considerations further influence organizational adoption. High-throughput networks and resource-constrained environments require efficient detection algorithms and architectures. Research investigated optimization techniques, parallel processing, and hierarchical detection models to address performance bottlenecks. Energy efficiency and computational overhead were also considered, particularly in distributed and embedded systems [77], [78].

Finally, research addressed the limitations and future directions of intrusion detection and prevention. Persistent challenges include encrypted traffic analysis, insider threat detection, adaptive adversaries, and the balance between automation and human oversight. While no single model provides comprehensive protection, the literature suggests that layered, hybrid, and context-aware approaches offer the greatest potential for enhancing organizational cyber defense [79], [80].

In summary, the literature presents a rich and diverse set of intrusion detection and prevention models. These models vary in detection paradigms, analytical techniques, architectural designs, and organizational applicability. Understanding their strengths and limitations is essential for designing effective cyber defense strategies that can adapt to evolving threats and organizational constraints.

## III. CONCEPTUAL FRAMEWORK FOR INTRUSION DETECTION AND PREVENTION IN ORGANIZATIONAL CYBER DEFENSE

The effectiveness of intrusion detection and prevention within organizations depends on more than the technical accuracy of detection algorithms. It is shaped by the interaction between detection models, system architecture, organizational processes, and human decision making. Building on the reviewed literature, this study proposes a conceptual framework that positions intrusion detection and prevention as an integrated, adaptive cyber defense capability embedded within the broader organizational security ecosystem.

At the core of the framework is the assumption that cyber defense effectiveness emerges from the continuous interaction between threat observation, analysis and classification, response execution, and organizational learning. Intrusion detection systems serve as the primary mechanism for observing and interpreting security-relevant events, while intrusion prevention mechanisms operationalize decisions through automated or semi-automated responses. These functions are not isolated; rather, they form a feedback-driven cycle in which detection outcomes inform prevention strategies, and prevention outcomes refine detection models over time.

The first component of the framework is the data acquisition and monitoring layer, which encompasses network traffic, host activity, application logs, and user behavior. Organizational environments are heterogeneous, containing legacy systems, cloud platforms, mobile devices, and third-party services. The framework therefore assumes multi-source data collection across network-based and host-based sensors [81], [82]. The completeness and quality of this data directly influence detection performance, particularly for anomaly-based and learning-driven models.

The second component is the analysis and detection layer, where intrusion detection models operate. This layer includes signature-based, anomaly-based, specification-based, and hybrid detection mechanisms. Signature-based detection provides reliable identification of known threats, while anomaly-based and behavioral models contribute adaptability by identifying deviations from expected patterns [83], [84]. Hybrid approaches are emphasized in the framework because they balance precision and generalization, reducing false positives while retaining sensitivity to novel attacks. Machine learning models, when applied at this layer, are treated as decision-support tools rather than autonomous arbiters, reflecting organizational concerns regarding explainability and trust [85].

The third component is the decision and response layer, which translates detection outcomes into preventive or corrective actions. In IPS-enabled environments, this may involve blocking traffic, terminating sessions, isolating hosts, or updating access control rules [86], [87]. The framework recognizes that not all detections should trigger automated responses. Instead, response strategies are conditioned on confidence levels, asset criticality, and potential operational impact. This aligns with findings in the literature that overly aggressive prevention can disrupt legitimate activity and undermine organizational confidence in security systems [88].

The fourth component is the organizational integration layer, which situates IDS and IPS within governance, policy, and incident response structures. Detection and prevention systems must align with security policies, compliance obligations, and risk management frameworks. Alerts and logs generated by IDS and IPS feed into incident response workflows, forensic analysis, and reporting mechanisms. Human analysts play a critical role in validating alerts, investigating incidents, and adapting detection rules, highlighting the socio-technical nature of cyber defense [89].

Finally, the framework incorporates a learning and adaptation layer. Intrusion detection and prevention are treated as evolving capabilities rather than static tools. Feedback from incidents, false positives, and changing threat patterns informs model retraining, signature updates, and policy adjustments. This adaptive loop is particularly important for addressing advanced persistent threats and insider attacks, which often evade single-layer defenses [90], [91]. Through continuous learning, the organization enhances its defensive posture over time.

Together, these components form a holistic conceptual framework that emphasizes integration, adaptability, and organizational alignment. Rather than focusing solely on algorithmic performance, the framework underscores that intrusion detection and prevention effectiveness arises from coordinated technical and organizational processes.

## IV. METHODOLOGY

This study adopts a conceptual and analytical methodology based on a structured synthesis of existing literature on intrusion detection and prevention models. Given the objective of evaluating and consolidating knowledge developed, the methodology does not involve empirical experimentation or system implementation. Instead, it follows a qualitative, theory-building approach suitable for developing integrative frameworks in cybersecurity research.

The methodology begins with a systematic identification of relevant studies on intrusion detection systems, intrusion prevention systems, machine learning-based detection, architectural models, and organizational security practices. Peer-reviewed journal articles, conference proceedings, technical reports, and authoritative standards were considered, provided they contributed to understanding detection models, prevention mechanisms, or their deployment in organizational contexts. Studies focusing solely on cryptographic protocols or unrelated aspects of information security were excluded.

Following identification, the literature was categorized according to key dimensions, including detection paradigm, system architecture, analytical technique, response strategy, and organizational integration. This thematic classification enabled comparison across approaches and facilitated identification of recurring patterns, strengths, and limitations. Particular attention was paid to studies that examined IDS and IPS performance in operational or organizational settings, as these provided insight into practical challenges beyond theoretical accuracy metrics.

The synthesis process involved iterative analysis, where insights from one category informed interpretation of others. For example, findings on false-positive rates in anomaly detection were examined alongside studies on alert fatigue and analyst workload to understand organizational implications [92], [93]. Similarly, architectural discussions were linked to scalability and governance considerations. Through this integrative analysis, the conceptual framework presented in Section 3 was developed as an abstraction that captures common principles across diverse models.

This methodology is appropriate for the study’s objective of advancing conceptual understanding rather than proposing new detection algorithms. By grounding the framework in established research, the study ensures theoretical consistency and relevance for organizations seeking to enhance cyber defense using proven intrusion detection and prevention models.

## V. DISCUSSION

The conceptual framework developed in this paper highlights that intrusion detection and prevention effectiveness cannot be attributed solely to the sophistication of detection algorithms. Instead, effectiveness emerges from the alignment of technical capabilities with organizational processes, governance structures, and human expertise. This observation is consistent with a substantial body of literature emphasizing that security technologies are embedded within socio-technical systems [94], [95].

One key implication of the framework is the importance of hybrid detection strategies [96], [97].

The literature demonstrates that no single detection paradigm is sufficient to address the diversity of cyber threats faced by organizations. Signature-based systems remain indispensable for detecting known attacks efficiently, while anomaly-based and behavioral models provide adaptability against evolving threats [98]. Organizations that rely exclusively on one approach risk blind spots or operational overload. The framework therefore supports layered detection architectures that combine complementary techniques.

Another important discussion point concerns automation versus human oversight. Intrusion prevention systems offer powerful capabilities for real-time response, but their effectiveness depends on careful calibration [99], [100]. Automated blocking based on uncertain detections can disrupt critical services, particularly in complex organizational environments. The framework supports a graduated response model in which high-confidence detections trigger automated actions, while ambiguous cases are escalated to human analysts. This approach reflects empirical findings that human judgment remains essential for contextual interpretation and strategic decision making [101], [102].

The framework also underscores the role of organizational learning in cyber defense. Many IDS and IPS deployments fail to improve over time because feedback from incidents and false alarms is not systematically incorporated into model updates or policy revisions. By explicitly including a learning and adaptation layer, the framework aligns with research on continuous security improvement and adaptive defense strategies [103], [104]. This perspective is particularly relevant in addressing long-term threats that unfold gradually and evade static detection rules [105], [106].

From a practical standpoint, the framework suggests that organizations should evaluate IDS and IPS investments not only in terms of detection accuracy but also in terms of integration, usability, and maintainability. Systems that generate excessive alerts or lack transparency may be underutilized or ignored, reducing their defensive value. Conversely, systems that align with organizational workflows and analyst capabilities are more likely to enhance overall cyber resilience.

## VI. CONCLUSION

This paper has examined intrusion detection and prevention models as foundational components of organizational cyber defense. Through a comprehensive review of research developed, it has highlighted the evolution of detection paradigms, architectural designs, analytical techniques, and organizational considerations that shape the effectiveness of IDS and IPS deployments. The study demonstrates that while significant technical progress has been made, challenges related to false positives, scalability, interpretability, and organizational integration persist.

The conceptual framework proposed in this paper provides a structured lens for understanding how intrusion detection and prevention contribute to cyber defense effectiveness. By emphasizing data acquisition, detection and analysis, response mechanisms, organizational integration, and continuous learning, the framework moves beyond algorithm-centric perspectives and captures the socio-technical nature of cybersecurity. It reinforces the view that effective cyber defense arises from coordinated technical systems and human processes rather than isolated tools.

For organizations, the findings suggest that enhancing cyber defense requires balanced investment in technology, people, and processes. Intrusion detection and prevention systems should be selected and configured in ways that align with organizational risk profiles, operational constraints, and governance structures. For researchers, the framework offers a basis for future empirical studies that examine how different configurations of IDS and IPS influence security outcomes in real-world environments.

In conclusion, intrusion detection and prevention models remain indispensable in organizational cybersecurity. Their effectiveness, however, depends on thoughtful integration, adaptive learning, and alignment with organizational context. By consolidating existing knowledge and presenting an integrative framework, this paper contributes to a deeper understanding of how IDS and IPS can enhance organizational cyber defense effectiveness in an evolving threat landscape.

## REFERENCES

[1] Abba Adam, Norhayati Zakuan, Salisu Alh. Uba Ado A. Bichi. Usman Shettima, Saif, Ali M., and Rajeh Bati Almasradi, “Supply Chain Sustainability Practices of Oil Servicing Firms in the Downstream Sector of Nigeria’s Oil and Gas Industry,” *Journal of Economic Info*, vol. 6, no. 4, pp. 11–14, Nov. 2019, doi: 10.31580/JEI.V6I4.1031.

[2] J. Cai and N. Li, “Growth Through Inter-sectoral Knowledge Linkages,” *Rev Econ Stud*, vol. 86, no. 5, pp. 1827–1866, Oct. 2019, doi: 10.1093/RESTUD/RDY062.

[3] S. A. Shah, D. Z. Seker, S. Hameed, and D. Draheim, “The rising role of big data analytics and IoT in disaster management: Recent advances, taxonomy and prospects,” *IEEE Access*, vol. 7, pp. 54595–54614, 2019, doi: 10.1109/ACCESS.2019.2913340.

[4] N. Kozodoi, S. Lessmann, K. Papakonstantinou, Y. Gatsoulis, and B. Baesens, “A multi-objective approach for profit-driven feature selection in credit scoring,” *Decis Support Syst*, vol. 120, pp. 106–117, May 2019, doi: 10.1016/J.DSS.2019.03.011.

[5] Y. Luo, H.-H. Tseng, L. Wei, and R. K. Ten Haken, “Balancing accuracy and interpretability of machine learning approaches for radiation treatment outcomes modeling,” 2019, doi: 10.1259/bjro.20190021.

[6] M. P. Papazoglou and A. S. Andreou, “Smart connected digital factories: Unleashing the power of industry 4.0,” *Communications in Computer and Information Science*, vol. 1073, pp. 77–101, 2019, doi: 10.1007/978-3-030-29193-8_5/FIGURES/4.

[7] A. Bruck, “Artificial Intelligence in rural offgrid Polygeneration Systems: : A Case Study with RVE.Sol focusing on Electricity Supply &amp;amp; Demand Balancing,” 2019, Accessed: May 13, 2019. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-264246

[8] D. Vance *et al.*, “Estimation of and barriers to waste heat recovery from harsh environments in industrial processes,” *J Clean Prod*, vol. 222, pp. 539–549, Jun. 2019, doi: 10.1016/J.JCLEPRO.2019.03.011.

[9] L. V. Pavão, C. B. B. Costa, and M. A. S. S. Ravagnani, “A new framework for work and heat exchange network synthesis and optimization,” *Energy Convers Manag*, vol. 183, pp. 617–632, Mar. 2019, doi: 10.1016/J.ENCONMAN.2019.01.018.

[10] R. Blaga, A. Sabadus, N. Stefu, C. Dughir, M. Paulescu, and V. Badescu, “A current perspective on the accuracy of incoming solar energy forecasting,” *Prog Energy Combust Sci*, vol. 70, pp. 119–144, Jan. 2019, doi: 10.1016/J.PECS.2018.10.003.

[11] U. R. Karmarkar and H. Plassmann, “Consumer Neuroscience: Past, Present, and Future,” *Organ Res Methods*, vol. 22, no. 1, pp. 174–195, Jan. 2019, doi: 10.1177/1094428117730598/ASSET/426D9139-D69C-47B8-83E4-A8D2E194FF44/ASSETS/IMAGES/LARGE/10.1177_1094428117730598-FIG1.JPG.

[12] A. Sieja *et al.*, “Optimization Sprints: Improving Clinician Satisfaction and Teamwork by Rapidly Reducing Electronic Health Record Burden,” *Mayo Clin Proc*, vol. 94, no. 5, pp. 793–802, May 2019, doi: 10.1016/J.MAYOCP.2018.08.036.

[13] D. E. Caughlin and T. N. Bauer, “Data visualizations and human resource management: The state of science and practice,” *Research in Personnel and Human Resources Management*, vol. 37, pp. 89–132, 2019, doi: 10.1108/S0742-730120190000037004/FULL/EPUB.

[14] S. L. Jordan, A. Wihler, W. A. Hochwarter, and G. R. Ferris, “The roles of grit in human

resources theory and research," *Research in Personnel and Human Resources Management*, vol. 37, pp. 53–88, 2019, doi: 10.1108/S0742-730120190000037003/FULL/HTML.

[15] B. R. Dineen, G. Van Hoye, F. Lievens, and L. M. Rosokha, "Third party employment branding: What are its signaling dimensions, mechanisms, and sources?," *Research in Personnel and Human Resources Management*, vol. 37, pp. 173–226, 2019, doi: 10.1108/S0742-730120190000037006/FULL/HTML.

[16] J. Capitano, K. L. McAlpine, and J. H. Greenhaus, "Organizational influences on work–home boundary permeability: A multidimensional perspective," *Research in Personnel and Human Resources Management*, vol. 37, pp. 133–172, 2019, doi: 10.1108/S0742-730120190000037005/FULL/HTML.

[17] N. Moonen, J. Baijens, M. Ebrahim, and R. Helms, "Small Business, Big Data: An Assessment Tool for (Big) Data Analytics Capabilities in SMEs," *Academy of Management Proceedings*, vol. 2019, no. 1, p. 16354, Aug. 2019, doi: 10.5465/AMBPP.2019.16354ABSTRACT.

[18] C. Lou and S. Yuan, "Influencer Marketing: How Message Value and Credibility Affect Consumer Trust of Branded Content on Social Media," *Journal of Interactive Advertising*, vol. 19, no. 1, pp. 58–73, Jan. 2019, doi: 10.1080/15252019.2018.1533501.

[19] A. E. Aiello, A. Renson, and P. N. Zivich, "Social media- and internet-based disease surveillance for public health," *Annu Rev Public Health*, vol. 41, pp. 101–118, Apr. 2019, doi: 10.1146/ANNUREV-PUBLHEALTH-040119-094402.

[20] L. Wu, Y. Zhi, Z. Sui, and Y. Liu, "Intra-urban human mobility and activity transition: Evidence from social media check-in data," *PLoS One*, vol. 9, no. 5, May 2014, doi: 10.1371/journal.pone.0097010.

[21] L. Li, L. Yang, H. Zhu, and R. Dai, "Explorative Analysis of Wuhan Intra-Urban Human Mobility Using Social Media Check-In Data," *PLoS One*, vol. 10, no. 8, p. e0135286, Aug. 2015, doi: 10.1371/JOURNAL.PONE.0135286',.

[22] Y. Liu, Z. Sui, C. Kang, and Y. Gao, "Uncovering Patterns of Inter-Urban Trip and Spatial Interaction from Social Media Check-In Data," *PLoS One*, vol. 9, no. 1, 2014.

[23] P. Alexopoulos and M. Wallace, "Creating domain-specific semantic lexicons for aspect-based sentiment analysis," *Proceedings - 10th International Workshop on Semantic and Social Media Adaptation and Personalization, SMAP 2015*, pp. 71–75, Dec. 2015, doi: 10.1109/SMAP.2015.7370083.

[24] B. J. Keegan and J. Rowley, "Evaluation and decision making in social media marketing," *emerald.com*, vol. 55, no. 1, pp. 15–31, 2017, doi: 10.1108/MD-10-2015-0450/FULL/HTML.

[25] H. Allcott and M. Gentzkow, "Social media and fake news in the 2016 election," *Journal of Economic Perspectives*, vol. 31, no. 2, pp. 211–236, Mar. 2017, doi: 10.1257/JEP.31.2.211.

[26] R. Ghandour, "Multimodal social media product reviews and ratings in e-commerce: an empirical approach," 2018.

[27] S. Aral, C. Dellarocas, and D. Godes, "Social media and business transformation: A Framework for research," *Information Systems Research*, vol. 24, no. 1, pp. 3–13, 2013, doi: 10.1287/ISRE.1120.0470.

[28] L. Li, L. Yang, H. Zhu, and R. Dai, "Explorative Analysis of Wuhan Intra-Urban Human Mobility Using Social Media Check-In Data," *PLoS One*, vol. 10, no. 8, p. e0135286, Aug. 2015, doi: 10.1371/JOURNAL.PONE.0135286.

[29] L. Phillips, C. Dowling, K. Shaffer, N. Hodas, and S. Volkova, "Using Social Media to Predict the Future: A Systematic Literature Review," Jun. 2017, Accessed: May 11, 2018. [Online]. Available: https://arxiv.org/pdf/1706.06134

[30] R. Crichton, D. Moodley, A. Pillay, R. Gakuba, and C. J. Seebregts, "An architecture and reference implementation of an open health information mediator: Enabling interoperability in the Rwandan health information exchange," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7789 LNCS, pp. 87–104, 2013, doi: 10.1007/978-3-642-39088-3_6.

[31] A. P. Monteiro, A. M. Soares, and O. L. Rua, "Entrepreneurial orientation and export performance: the mediating effect of organisational resources and dynamic capabilities," *J. for International Business and Entrepreneurship Development*, vol. 10, no. 1, p. 3, 2017, doi: 10.1504/JIBED.2017.082749.

[32] N. A. Abu Seman *et al.*, "The mediating effect of green innovation on the relationship between green supply chain management and environmental performance," *J Clean Prod*, vol. 229, pp. 115–127, Aug. 2019, doi: 10.1016/j.jclepro.2019.03.211.

[33] Ratnawati, B. E. Soetjipto, F. D. Murwani, and H. Wahyono, "The Role of SMEs' Innovation and Learning Orientation in Mediating the Effect of CSR Programme on SMEs' Performance and Competitive Advantage," *Global Business Review*, vol. 19, no. 3_suppl, pp. S21–S38, Jun. 2018, doi: 10.1177/0972150918757842.

[34] H. Liu, "The research of information disseminating system management in new media age," *Lecture Notes in Electrical Engineering*, vol. 241 LNEE, no. VOL. 1, pp. 249–258, 2014, doi: 10.1007/978-3-642-40078-0_21.

[35] C. Alvez, E. Miranda, G. Etchart, and S. Ruiz, "Efficient Iris Recognition Management in Object-Related Databases," *J Comput Sci Technol*, vol. 18, no. 02, p. e12, Oct. 2018, doi: 10.24215/16666038.18.E12.

[36] A. Sharma and P. Kaur, "A Multitenant Data Store Using a Column Based NoSQL Database," *2019 12th International Conference on Contemporary Computing, IC3 2019*, Aug. 2019, doi: 10.1109/IC3.2019.8844906.

[37] A. Geissbuhler *et al.*, "Trustworthy reuse of health data: A transnational perspective," *Int J Med Inform*, vol. 82, no. 1, pp. 1–9, Jan. 2013, doi: 10.1016/J.IJMEDINF.2012.11.003.

[38] S. C. Y. L. X Hu, "Optimization of FMCG supply chain by using data-driven methods," *J Intell Manuf*, vol. 30, no. 1, pp. 81–92, 2019.

[39] Y. Song, R. Routray, R. Jain, and C. H. Tan, "A data-driven storage recommendation service for multitenant storage management environments," *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, pp. 1026–1040, Jun. 2015, doi: 10.1109/INM.2015.7140429.

[40] J. L. L. T. T Wang, "Data-driven fast moving consumer goods supply chain model and application," *Int J Control Autom*, vol. 11, no. 5, pp. 125–138, 2018.

[41] J. L. Y. G. DD Ni, "A comparative study of physics-based and data-driven models for predictive maintenance," *Mech Syst Signal Process*, vol. 119, pp. 538–550, 2019.

[42] J. Sandefur and A. Glassman, "The Political Economy of Bad Data: Evidence from African Survey and Administrative Statistics," *Journal of Development Studies*, vol. 51, no. 2, pp. 116–132, Feb. 2015, doi: 10.1080/00220388.2014.968138.

[43] A. Castleberry and A. Nolen, "Thematic analysis of qualitative research data: Is it as easy as it sounds?," *Curr Pharm Teach Learn*,

vol. 10, no. 6, pp. 807–815, Jun. 2018, doi: 10.1016/J.CPTL.2018.03.019.

[44] K. Witkowski, "Internet of Things, Big Data, Industry 4.0 - Innovative Solutions in Logistics and Supply Chains Management," *Procedia Eng*, vol. 182, pp. 763–769, 2017, doi: 10.1016/j.proeng.2017.03.197.

[45] A. Kaushik and A. Raman, "The new data-driven enterprise architecture for e-healthcare: Lessons from the indian public sector," *Gov Inf Q*, vol. 32, no. 1, pp. 63–74, 2015, doi: 10.1016/J.GIQ.2014.11.002.

[46] J. Wang, S. Das, R. Rai, and C. Zhou, "Data-driven simulation for fast prediction of pull-up process in bottom-up stereo-lithography," *CAD Computer Aided Design*, vol. 99, pp. 29–42, Jun. 2018, doi: 10.1016/J.CAD.2018.02.002.

[47] D. Li, W. Daamen, and R. M. P. Goverde, "Estimation of train dwell time at short stops based on track occupation event data: A study at a Dutch railway station," *J Adv Transp*, vol. 50, no. 5, pp. 877–896, Aug. 2016, doi: 10.1002/ATR.1380.

[48] S. Rosenbaum, "Data governance and stewardship: Designing data stewardship entities and advancing data access," *Health Serv Res*, vol. 45, no. 5 PART 2, pp. 1442–1455, Oct. 2010, doi: 10.1111/J.1475-6773.2010.01140.X.

[49] H. Li, L. Xiong, L. Zhang, and X. Jiang, "DPSynthesizer: Differentially private data synthesizer for privacy preserving data sharing," *Proceedings of the VLDB Endowment*, vol. 7, no. 13, pp. 1677–1680, 2014, doi: 10.14778/2733004.2733059.

[50] V. Khatri and C. V. Brown, "Designing data governance," *Commun ACM*, vol. 53, no. 1, pp. 148–152, Jan. 2010, doi: 10.1145/1629175.1629210.

[51] S. O'Riain, E. Curry, and A. Harth, "XBRL and open data for global financial ecosystems: A linked data approach," *International Journal of Accounting Information Systems*, vol. 13, no. 2, pp. 141–162, Jun. 2012, doi: 10.1016/J.ACCINF.2012.02.002.

[52] M. Kim, J. Jeong, and S. Bae, "Demand forecasting based on machine learning for mass customization in smart manufacturing," *ACM International Conference Proceeding Series*, pp. 6–11, Apr. 2019, doi: 10.1145/3335656.3335658.

[53] M. A. Gianfrancesco, S. Tamang, J. Yazdany, and G. Schmajuk, "Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data," *JAMA Intern Med*, vol. 178, no. 11, pp. 1544–1547, Nov. 2018, doi: 10.1001/JAMAINTERNMED.2018.3763.

[54] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," *J Med Internet Res*, vol. 20, no. 5, May 2018, doi: 10.2196/10059.

[55] S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," *Journal of Organizational Computing and Electronic Commerce*, vol. 28, no. 3, pp. 269–282, Jul. 2018, doi: 10.1080/10919392.2018.1484598.

[56] N. M. Radziwill and M. C. Benton, "Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management," Jul. 2017, Accessed: Dec. 20, 2017. [Online]. Available: http://arxiv.org/abs/1707.02653

[57] N. Kammoun, A. Bounfour, A. Özaygen, and R. Dieye, "Financial market reaction to cyberattacks," *Cogent Economics and Finance*, vol. 7, no. 1, 2019, doi: 10.1080/23322039.2019.1645584.

[58] "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Apr. 2018, doi: 10.6028/NIST.CSWP.04162018.

[59] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *Journal of Information Security and Applications*, vol. 42, pp. 36–45, Oct. 2018, doi: 10.1016/J.JISA.2018.08.002.

[60] N. A. Hashim, Z. Z. Abidin, N. A. Zakaria, R. Ahmad, and A. P. Puvanasvaran, “Risk assessment method for insider threats in cyber security: A review,” *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, pp. 126–130, 2018, doi: 10.14569/IJACSA.2018.091119.

[61] K. Renaud, S. Flowerday, M. Warkentin, P. Cockshott, and C. Orgeron, “Is the responsibilization of the cyber security risk reasonable and judicious?,” *Comput Secur*, vol. 78, pp. 198–211, Sep. 2018, doi: 10.1016/J.COSE.2018.06.006.

[62] A. Alvarenga and G. Tanev, “A Cybersecurity Risk Assessment Framework that Integrates Value-Sensitive Design,” *Technology Innovation Management Review*, vol. 7, no. 4, pp. 32–43, Apr. 2017, doi: 10.22215/TIMREVIEW/1069.

[63] L. Coventry and D. Branley, “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,” *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/J.MATURITAS.2018.04.008.

[64] G. Collard, S. Ducroquet, E. Disson, and G. Talens, “A definition of Information Security Classification in cybersecurity context,” *Proceedings - International Conference on Research Challenges in Information Science*, pp. 77–82, Jun. 2017, doi: 10.1109/RCIS.2017.7956520.

[65] H. Alami, M. P. Gagnon, M. A. Ag Ahmed, and J. P. Fortin, “Digital health: Cybersecurity is a value creation lever, not only a source of expenditure,” *Health Policy Technol*, vol. 8, no. 4, pp. 319–321, Dec. 2019, doi: 10.1016/J.HLPT.2019.09.002.

[66] L. A. Saxon, N. Varma, L. M. Epstein, L. I. Ganz, and A. E. Epstein, “Factors influencing the decision to proceed to firmware upgrades to implanted pacemakers for cybersecurity risk mitigation,” *Circulation*, vol. 138, no. 12, pp. 1274–1276, 2018, doi: 10.1161/CIRCULATIONAHA.118.034781.

[67] M. Y. Ilchenko, L. A. Uryvsky, and A. V. Moshinskaya, “Developing telecommunication strategies based on scenarios in the information community,” *Cybern. Syst. Analysis*, vol. 53, no. 6, pp. 905–913, Nov. 2017, doi: 10.1007/s10559-017-9992-9.

[68] V. Y. Meytus, “Problems of constructing intelligent systems. Knowledge representation,” *Cybern. Syst. Analysis*, vol. 55, no. 4, pp. 521–530, Jul. 2019, doi: 10.1007/s10559-019-00160-5.

[69] A. V. Palagin, “Functionally oriented approach in research-related design,” *Cybern. Syst. Analysis*, vol. 53, no. 6, pp. 986–992, Nov. 2017, doi: 10.1007/s10559-017-0001-0.

[70] I. G. Kryvonos, I. V. Krak, O. V. Barmak, and A. I. Kulias, “Methods to Create Systems for the Analysis and Synthesis of Communicative Information,” *Cybern Syst Anal*, vol. 53, no. 6, pp. 847–856, Nov. 2017, doi: 10.1007/S10559-017-9986-7.

[71] J. Wang, Y. Zhou, Y. Wang, J. Zhang, C. L. P. Chen, and Z. Zheng, “Multiobjective Vehicle Routing Problems with Simultaneous Delivery and Pickup and Time Windows: Formulation, Instances, and Algorithms,” *IEEE Trans Cybern*, vol. 46, no. 3, pp. 582–594, Mar. 2016, doi: 10.1109/TCYB.2015.2409837.

[72] L. Oneto *et al.*, “Dynamic delay predictions for large-scale railway networks: Deep and shallow extreme learning machines tuned via thresholdout,” *IEEE Trans Syst Man Cybern Syst*, vol. 47, no. 10, pp. 2754–2767, Oct. 2017, doi: 10.1109/TSMC.2017.2693209.

[73] Y. Zhang and B. Li, “A Novel Software Defined Networking Framework for Cloud Environments,” *Proceedings - 3rd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2016 and 2nd IEEE International Conference of Scalable and Smart Cloud, SSC 2016*, pp. 30–35, Aug. 2016, doi: 10.1109/CSCLOUD.2016.22.

[74] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/J.MATURITAS.2018.04.008;

[75] M. Choi and W. E. A. Ruona, "Individual readiness for organizational change and its implications for human resource and organization development," *Human Resource Development Review*, vol. 10, no. 1, pp. 46–73, Mar. 2011, doi: 10.1177/1534484310384957.

[76] J. Pfeffer, "Fighting the war for talent is hazardous to your organization's health," *Organ Dyn*, vol. 29, no. 4, pp. 248–259, Mar. 2001, doi: 10.1016/S0090-2616(01)00031-6.

[77] B. J. L. Berry, L. D. Kiel, and E. Elliott, "Adaptive agents, intelligence, and emergent human organization: Capturing complexity through agent-based modeling," *Proc Natl Acad Sci U S A*, vol. 99, no. SUPPL. 3, pp. 7187–7188, May 2002, doi: 10.1073/PNAS.092078899.

[78] M. Gaynor, K. Ho, and R. J. Town, "The Industrial Organization of Health-Care Markets," *J Econ Lit*, vol. 53, no. 2, pp. 235–284, Jun. 2015, doi: 10.1257/JEL.53.2.235<SPAN.

[79] M. Gaynor, K. Ho, and R. J. Town, "The industrial organization of health-care markets," *J Econ Lit*, vol. 53, no. 2, pp. 235–284, Jun. 2015, doi: 10.1257/JEL.53.2.235.

[80] G. M. Grossman and E. Helpman, "Managerial incentives and the international organization of production," *J Int Econ*, vol. 63, no. 2, pp. 237–262, Jul. 2004, doi: 10.1016/S0022-1996(03)00072-2.

[81] S. Chanias, M. D. Myers, and T. Hess, "Digital transformation strategy making in pre-digital organizations: The case of a financial services provider," *Journal of Strategic Information Systems*, vol. 28, no. 1, pp. 17–33, Mar. 2019, doi: 10.1016/J.JSIS.2018.11.003.

[82] C. M. Olszak, "Toward Better Understanding and Use of Business Intelligence in Organizations," *Information Systems Management*, vol. 33, no. 2, pp. 105–123, Apr. 2016, doi: 10.1080/10580530.2016.1155946.

[83] T. J. Sturgeon, "Modular production networks: A new American model of industrial organization," *Industrial and Corporate Change*, vol. 11, no. 3, pp. 451–496, 2002, doi: 10.1093/ICC/11.3.451.

[84] K. Walshe and S. M. Shortell, "When Things Go Wrong: How Health Care Organizations Deal With Major Failures," *Health Aff*, vol. 23, no. 3, pp. 103–111, May 2004, doi: 10.1377/hlthaff.23.3.103.

[85] J. Abelson, K. Li, G. Wilson, K. Shields, C. Schneider, and S. Boesveld, "Supporting quality public and patient engagement in health system organizations: development and usability testing of the Public and Patient Engagement Evaluation Tool," *Health Expect*, vol. 19, no. 4, pp. 817–827, Aug. 2016, doi: 10.1111/HEX.12378.

[86] D. W. Roblin, T. K. Houston, J. J. Allison, P. J. Joski, and E. R. Becker, "Disparities in Use of a Personal Health Record in a Managed Care Organization," *Journal of the American Medical Informatics Association*, vol. 16, no. 5, pp. 683–689, Sep. 2009, doi: 10.1197/jamia.M3169.

[87] K. Zhu and K. L. Kraemer, "Post-adoption variations in usage and value of e-business by organizations: Cross-country evidence from the retail industry," *Information Systems Research*, vol. 16, no. 1, pp. 61–84, 2005, doi: 10.1287/ISRE.1050.0045.

[88] O. Tamburis, M. Mangia, M. Contenti, G. Mercurio, and A. R. Mori, "The LITIS conceptual framework: Measuring eHealth readiness and adoption dynamics across the Healthcare Organizations," *Health Technol (Berl)*, vol. 2, no. 2, pp. 97–112, Jun. 2012, doi: 10.1007/S12553-012-0024-5.

[89] M. Sajid and K. Ahsan, "ROLE OF ENTERPRISE ARCHITECTURE IN HEALTHCARE ORGANIZATIONS AND KNOWLEDGE-BASED MEDICAL DIAGNOSIS SYSTEM," *Journal of Information Systems and Technology Management*, vol. 13, no. 2, pp. 181–192, Sep. 2016, doi: 10.4301/S1807-17752016000200002;

[90] A. Alibrahim and S. Wu, "An agent-based simulation model of patient choice of health care providers in accountable care organizations," *Health Care Manag Sci*, vol. 21, no. 1, pp. 131–143, Mar. 2018, doi: 10.1007/S10729-016-9383-1.

[91] B. Weiner, "A theory of organizational readiness for change," *Implement Sci*, vol. 4, 2009.

[92] M. Arena and G. Azzone, "Identifying Organizational Drivers of Internal Audit Effectiveness," *International Journal of Auditing*, vol. 13, no. 1, pp. 43–60, Mar. 2009, doi: 10.1111/J.1099-1123.2008.00392.X.

[93] M. A. Kareem and A. A. A. Alameer, "The impact of dynamic capabilities on organizational effectiveness," *Management and Marketing*, vol. 14, no. 4, pp. 402–418, Dec. 2019, doi: 10.2478/MMCKS-2019-0028.

[94] D. Holt, H. Feild, S. Harris, A. Armenakis, H. Feild, and S. Harris, "Readiness for Organizational Change—The Systematic Development of a Scale," *J Appl Behav Sci*, vol. 43, no. 2, 2007.

[95] L. M. Fonseca and J. P. Domingues, "The best of both worlds? Use of Kaizen and other continuous improvement methodologies within Portuguese ISO 9001 certified organizations," *TQM Journal*, vol. 30, no. 4, pp. 321–334, Jul. 2018, doi: 10.1108/TQM-12-2017-0173.

[96] M. Augier and D. J. Teece, "Dynamic capabilities and the role of managers in business strategy and economic performance," *Organization Science*, vol. 20, no. 2, pp. 410–421, Mar. 2009, doi: 10.1287/ORSC.1090.0424.

[97] V. A. Assenova and O. Sorenson, "Legitimacy and the benefits of firm formalization," *Organization Science*, vol. 28, no. 5, pp. 804–818, 2017, doi: 10.1287/ORSC.2017.1146.

[98] T. Heinze, P. Shapira, J. D. Rogers, and J. M. Senker, "Organizational and institutional influences on creativity in scientific research," *Res Policy*, vol. 38, no. 4, pp. 610–623, May 2009, doi: 10.1016/J.RESPOL.2009.01.014.

[99] C. Shea, S. Jacobs, D. Esserman, K. Bruce, and B. Weiner, "Organizational readiness for implementing change: a psychometric assessment of a new measure," *Implement Sci*, vol. 9, no. 1, 2014.

[100] R. Snyder-Halpern, "Indicators of organizational readiness for clinical information technology/systems innovation: A Delphi study," *Int J Med Inform*, vol. 63, no. 3, pp. 179–204, 2001, doi: 10.1016/S1386-5056(01)00179-4.

[101] L. Agostini and R. Filippini, "Organizational and managerial challenges in the path toward Industry 4.0," *European Journal of Innovation Management*, vol. 22, no. 3, pp. 406–421, May 2019, doi: 10.1108/EJIM-02-2018-0030.

[102] A. Lopez-Cabrales, R. Valle, and I. Herrero, "The contribution of core employees to organizational capabilities and efficiency," *Hum Resour Manage*, vol. 45, no. 1, pp. 81–109, Mar. 2006, doi: 10.1002/HRM.20094.

[103] S. L. Margolis and C. D. Hansen, "Visions to Guide Performance: A Typology of Multiple Future Organizational Images," *Performance Improvement Quarterly*, vol. 16, no. 4, pp. 40–58, Oct. 2008, doi: 10.1111/J.1937-8327.2003.TB00293.X.

[104] A. Gunasekaran *et al.*, "Big data and predictive analytics for supply chain and organizational performance," *J Bus Res*, vol. 70, pp. 308–317, Jan. 2017, doi: 10.1016/j.jbusres.2016.08.004.

[105] N. Melville, K. Kraemer, and V. Gurbaxani, "Information technology and organizational performance: An integrative model of IT business value," *MIS Q.*, vol. 28, no. 2, pp. 283–321, 2004, doi: 10.2307/25148636.

[106] M. Touré, L. Poissant, and B. R. Swaine, "Assessment of organizational readiness for e-health in a rehabilitation centre," *Disabil Rehabil*, vol. 34, no. 2, pp. 167–173, 2012, doi: 10.3109/09638288.2011.591885.