SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIES NO. 198

CYBERSECURITY ANALYTICS: LEVERAGING BUSINESS ANALYTICS IN INDUSTRY 4.0 SETTINGS

Radosław WOLNIAK

Silesian University of Technology, Organization and Management Department, Economics and Informatics Institute; rwolniak@polsl.pl, ORCID: 0000-0003-0317-9811

Purpose: The purpose of this publication is to present the applications of usage of business analytics in cybersecurity analytics.
Design/methodology/approach: Critical literature analysis. Analysis of international literature from main databases and polish literature and legal acts connecting with researched topic.
Findings: The integration of business analytics into cybersecurity practices within Industry 4.0 signifies a pivotal advancement in safeguarding organizational assets against the evolving cyber threat landscape. As industrial systems grow more complex and interconnected, traditional security methods focused on perimeter defenses are increasingly inadequate. Modern cybersecurity strategies must therefore incorporate advanced analytics to manage and mitigate risks effectively. Business analytics enhances cybersecurity through sophisticated machine learning algorithms, predictive capabilities for anticipating future threats, and improved incident response via real-time monitoring and automated alerts. These innovations foster a proactive and efficient security approach, enabling swift detection, response, and informed decision-making based on thorough risk assessments. Despite these advantages, challenges such as data overload, false positives, integration hurdles, and the need for specialized expertise persist. Additionally, concerns about data privacy, costs, and analytical complexity must be managed. Embracing business analytics while addressing these challenges will enable organizations to fortify their security posture, optimize resource use, and adapt to the demands of Industry 4.0, thereby shaping the future of cybersecurity in a rapidly evolving digital landscape.
Originality/Value: Detailed analysis of all subjects related to the problems connected with the usage of business analytics in the case of cybersecurity analytics.

Keywords: business analytics, Industry 4.0, digitalization, artificial intelligence, real-time monitoring; cybersecurity.
Category of the paper: literature review.

http://dx.doi.org/10.29119/1641-3466.2024.198.35

1. Introduction

As more devices and systems interact within complex industrial networks, the number of entry points for potential attacks increases. The traditional approach to security, which focused on protecting the perimeters of systems and networks, proves inadequate in the face of modern, distributed architectures. Cybercriminals exploit vulnerabilities not only in hardware and software but also within the dynamically evolving IT and operational technology (OT) environments.

In the context of Industry 4.0, cybersecurity analytics aims not only to identify threats but also to predict and prevent potential attacks. Modern analytical systems leverage advanced machine learning algorithms and artificial intelligence to process the vast amounts of data generated by devices and systems. This approach enables the detection of patterns and anomalies that may indicate security breaches. Such analytics not only allow for real-time monitoring and risk assessment but also facilitate the early detection of potential threats before they escalate into significant incidents.

The implementation of techniques like automated incident response has become indispensable. In the realm of Industry 4.0, where the speed of response can determine the extent of damage, automation enables swift and effective actions to mitigate the impact of incidents. Automated systems can isolate affected components, adjust network configurations, or initiate recovery procedures, thereby minimizing disruptions to industrial operations (Scappini, 2016).

In addition to technological aspects, understanding the human factor in managing security in the Industry 4.0 era is also crucial. Organizations must invest in training their personnel to ensure they are well-versed in the threats and defensive strategies. Effective management of risk and protection of resources requires collaboration between IT and OT teams, supported by appropriate policies and procedures. This holistic approach is essential for safeguarding the integrity and continuity of operations in an increasingly interconnected and complex industrial landscape.

The purpose of this publication is to present the applications of usage of business analytics in cybersecurity analytics.

2. The selected aspects of business analytics usage in cybersecurity analytics

Business analytics has increasingly become a critical component in the field of cybersecurity, offering powerful tools and methodologies to enhance the effectiveness of security measures. In particular, several aspects of business analytics play a pivotal role in optimizing cybersecurity strategies and operations.

One of the primary aspects of business analytics in cybersecurity is predictive analytics. By leveraging historical data and advanced statistical models, organizations can anticipate potential security threats before they manifest. Predictive analytics utilizes machine learning algorithms to identify patterns and anomalies in network traffic, user behavior, and system performance. This proactive approach allows cybersecurity teams to implement preventive measures and bolster defenses against emerging threats, rather than reacting to incidents after they occur.

Another crucial aspect is the use of risk analytics, which helps organizations assess and prioritize security risks based on their potential impact and likelihood. Risk analytics involves quantifying and evaluating vulnerabilities in the context of business operations and objectives. By analyzing factors such as asset value, threat landscape, and existing controls, risk analytics enables organizations to make informed decisions about where to allocate resources and which security measures to prioritize. This strategic approach ensures that security efforts are aligned with the overall business strategy and effectively mitigate the most significant risks (Akundi et al., 2022).

Business analytics enhances incident response and management through real-time monitoring and analysis. Security information and event management (SIEM) systems, which are integral to modern cybersecurity frameworks, utilize business analytics to collect, correlate, and analyze data from various sources (Ghibakholl et al., 2022). This real-time visibility allows cybersecurity teams to detect and respond to incidents swiftly, minimizing the potential impact on the organization. Advanced analytics tools can sift through vast amounts of log data and identify indicators of compromise, enabling quicker identification of breaches and more effective containment strategies (Gajdzik, Wolniak, 2022; Gajdzik et al., 2023).

Also business analytics contributes to improving threat intelligence by aggregating and analyzing data from diverse sources, including external threat feeds, social media, and industry reports. This comprehensive view enhances the understanding of the threat landscape and helps organizations stay ahead of emerging threats and trends (Bakir, Dahlan, 2022). By incorporating threat intelligence into their security strategies, organizations can better anticipate and prepare for sophisticated cyber attacks, ensuring a more resilient defense posture Cillo et al., 2022).

Business analytics supports continuous improvement in cybersecurity practices through performance measurement and benchmarking. By analyzing metrics such as incident response times, detection rates, and compliance levels, organizations can evaluate the effectiveness of their security measures and identify areas for enhancement. This data-driven approach facilitates ongoing optimization of cybersecurity processes and ensures that security investments deliver tangible benefits (Sułkowski, Wolniak, 2015, 2016, 2018; Wolniak, Skotnicka-Zasadzień, 2008, 2010, 2014, 2018, 2019, 2022; Gajdzik, Wolniak, 2023; Swarnakar et al., 2023).

Table 1 contains descriptions of how business analytics is used in the case of cybersecurity analytics.

Table 1.
The usage of business analytics in cybersecurity analytics

Aspect of cybersecurity analyticsg	**Description of Usage of Business Analytics**
Predictive Analytics	Business analytics utilize predictive models and machine learning algorithms to analyze historical data and identify patterns or anomalies that may indicate potential security threats. This approach allows organizations to anticipate and prepare for future cyber threats, improving their proactive defenses and reducing the likelihood of successful attacks.
Risk Analytics	Risk analytics involves assessing and quantifying vulnerabilities in the context of business operations. By analyzing asset values, threat landscapes, and existing controls, organizations can prioritize security measures based on the potential impact and likelihood of risks. This strategic approach ensures that resources are allocated effectively to mitigate the most significant risks.
Real-Time Monitoring	Business analytics are employed in real-time monitoring through Security Information and Event Management (SIEM) systems. These systems collect and analyze data from various sources to detect and respond to security incidents swiftly. Advanced analytics tools help identify indicators of compromise, enabling quicker responses and effective containment strategies.
Threat Intelligence	By aggregating and analyzing data from diverse sources such as external threat feeds, social media, and industry reports, business analytics enhance threat intelligence. This comprehensive analysis improves understanding of the threat landscape, helps anticipate emerging threats, and strengthens defensive measures against sophisticated cyber attacks.
Performance Measurement	Business analytics track and measure various cybersecurity metrics, including incident response times, detection rates, and compliance levels. Analyzing these metrics allows organizations to evaluate the effectiveness of their security measures, identify areas for improvement, and optimize cybersecurity processes to ensure better protection of critical assets.

Source: (Adel, 2022; Akundi et al., 2022; Olsen, 2023; Aslam, et al., 2020; Bakir, Dahlan, 2022; Cillo et al., 2022; Ghibakholl et al., 2022, Javaid, Haleem, 2020, Javaid et al., 2020; Cam et al., 2021; Charles et al., 2023; Greasley, 2019; Hurwitz et al., 2015; Nourani, 2021; Peter et al., 2023).

3. Software used in cybersecurity analytics analysis in Industry 4.0 conditions

The usage of business analytics software in cybersecurity analytics has become increasingly critical as organizations strive to protect their digital assets in a landscape of growing and evolving threats. These software solutions leverage advanced analytics, machine learning, and data integration techniques to enhance security operations and incident response capabilities.

One of the most prominent examples of business analytics software in this domain is Splunk. Known for its robust real-time data indexing and search capabilities, Splunk allows security teams to sift through vast amounts of machine-generated data to identify potential security threats. Its customizable dashboards and automated alerting features enable organizations to monitor their systems proactively and respond swiftly to anomalies or incidents accordingly (Jonek-Kowalska, Wolniak, 2021, 2022, 2023; Rosak-Szyrocka et al., 2023; Gajdzik et al., 2023; Jonek-Kowalska et al., 2022; Kordel, Wolniak, 2021; Orzeł, Ponomarenko et al., 2016; Stawiarska et al., 2020, 2021; Stecuła, Wolniak, 2022; Olkiewicz et al., 2021).

IBM QRadar is another key player, offering a comprehensive security intelligence and analytics platform. QRadar excels in correlating events from diverse sources to provide a unified view of security incidents. Its capabilities include real-time log management, advanced threat detection, and automated incident response, all of which are essential for managing complex threat landscapes and ensuring timely reactions to security breaches.

Sumo Logic provides a cloud-native solution for log management and analytics, which is particularly valuable for organizations operating in a cloud environment. Its real-time analytics and machine learning-based anomaly detection help organizations to gain insights into their security data efficiently. The scalability and flexibility of Sumo Logic make it a suitable choice for modern enterprises seeking to manage and analyze large volumes of data across various platforms.

Elastic Security, built on the Elastic Stack, integrates with existing systems to enhance threat detection and response. It offers a unified search and analytics platform that supports real-time data ingestion and advanced querying. The open-source nature of Elastic Security allows for extensive customization and integration, making it a versatile tool for detecting and mitigating threats in diverse IT environments.

LogRhythm is well-regarded for its centralized log management and advanced correlation features. It combines behavioral analytics with traditional SIEM capabilities to provide a comprehensive view of security events. LogRhythm's automated response features further streamline the process of addressing security incidents, enabling organizations to act quickly and reduce the potential impact of threats.

ArcSight, from Micro Focus, delivers a powerful SIEM solution with real-time event correlation and threat intelligence integration. Its comprehensive log management and compliance reporting functionalities support effective security monitoring and regulatory adherence. ArcSight's ability to correlate events from multiple sources helps organizations to identify and address security issues with greater accuracy.

Microsoft Sentinel, a cloud-native SIEM solution, integrates seamlessly with the Azure ecosystem to provide advanced threat detection and response capabilities. Sentinel leverages AI-driven analytics to enhance threat detection and automate incident management. Its scalability and integration with other Microsoft services make it a compelling choice for organizations leveraging cloud technologies.

Rapid7 InsightIDR offers a cloud-based solution focused on user behavior analytics and endpoint detection. Its automated response capabilities and extensive integrations with other security tools facilitate a proactive approach to threat detection and management. InsightIDR's emphasis on user behavior and endpoint visibility provides valuable insights into potential security risks and vulnerabilities.

ThreatConnect provides a threat intelligence platform designed to aggregate, analyze, and operationalize threat data. It supports threat-sharing and advanced analytics to enhance the understanding of the threat landscape. By integrating threat intelligence into security operations, ThreatConnect helps organizations stay ahead of emerging threats and improve their defensive strategies (Du et al., 2023; Fjellström, Osarenkhoe, 2023; Castro et al., 2014; Wang et al., 2023).

McAfee Enterprise Security Manager (ESM) provides a comprehensive SIEM solution that emphasizes real-time event correlation and customizable reporting. Its threat intelligence integration and automated response capabilities help organizations manage and respond to security threats effectively, ensuring robust protection for their digital assets (Adel., 2022).

Table 2 highlighting examples of software and applications used in cybersecurity analytics, along with descriptions of their usage.

Table 2.
The usage of business analytics software in cybersecurity analytics

Software/Application	Description	Key Features
Splunk	Splunk is a comprehensive platform for searching, monitoring, and analyzing machine-generated data in real-time.	Real-time data indexing, advanced search capabilities, customizable dashboards, and automated alerting.
IBM QRadar	IBM QRadar provides integrated security intelligence and analytics to detect and respond to cyber threats.	Log management, real-time correlation of events, advanced threat detection, and automated incident response.
Sumo Logic	Sumo Logic offers cloud-based log management and analytics to gain insights into application and security data.	Cloud-native architecture, real-time analytics, machine learning-based anomaly detection, and scalability.
Elastic Security	Elastic Security is an open-source solution that integrates with the Elastic Stack for threat detection and response.	Unified search and analytics, real-time data ingestion, advanced querying, and customizable visualizations.

Cont. table 2.

LogRhythm	LogRhythm provides security information and event management (SIEM) with advanced analytics for threat detection.	Centralized log management, advanced correlation, behavioral analytics, and automated response capabilities.
ArcSight	ArcSight, by Micro Focus, delivers SIEM solutions for identifying and responding to security threats.	Real-time event correlation, threat intelligence integration, comprehensive log management, and compliance reporting.
Microsoft Sentinel	Microsoft Sentinel is a cloud-native SIEM that leverages machine learning to provide threat detection and response.	Integration with Azure ecosystem, AI-driven threat detection, automated incident management, and scalable analytics.
Rapid7 InsightIDR	InsightIDR by Rapid7 is a cloud-based solution for threat detection and incident response, focusing on user behavior analytics.	User behavior analytics, endpoint detection, automated response, and extensive integrations with other security tools.
ThreatConnect	ThreatConnect offers a threat intelligence platform for aggregating, analyzing, and operationalizing threat data.	Threat intelligence aggregation, advanced analytics, threat-sharing capabilities, and integration with other security systems.
McAfee Enterprise Security Manager (ESM)	McAfee ESM provides a SIEM solution that helps organizations manage and respond to security threats effectively.	Real-time event correlation, customizable reporting, threat intelligence integration, and automated response capabilities.

Source: (Adel, 2022; Akundi et al., 2022; Olsen, 2023; Aslam, et al., 2020; Bakir, Dahlan, 2022; Cillo et al., 2022; Ghibakholl et al., 2022, Javaid, Haleem, 2020; Javaid et al., 2020; Cam et al., 2021; Charles et al., 2023; Greasley, 2019; Hurwitz et al., 2015; Nourani, 2021; Peter et al., 2023).

4. Advantages and problems of business analytics usage in cybersecurity analytics

The advantages of utilizing business analytics in cybersecurity analytics are substantial and multifaceted, contributing significantly to the effectiveness and efficiency of security operations. One of the foremost advantages is enhanced threat detection. Business analytics leverage sophisticated algorithms and machine learning techniques to analyze vast amounts of data from various sources. This capability allows organizations to identify patterns and anomalies that might indicate potential security threats more accurately and swiftly than traditional methods. By processing data in real-time, analytics tools can detect irregularities that could signal the presence of a cyber threat, thus improving the chances of catching potential issues before they escalate into serious incidents (Charles et al., 2023).

Predictive capabilities are another crucial benefit of business analytics in cybersecurity. By examining historical data and identifying trends, analytics can forecast future threats and vulnerabilities. This foresight enables organizations to implement preventive measures proactively, thereby reducing the likelihood of successful attacks. Predictive analytics transforms reactive security strategies into proactive ones, allowing organizations to stay ahead of emerging threats and safeguard their systems more effectively. Improved incident response is a significant advantage of integrating business analytics into cybersecurity practices. Real-time data analysis and automated alerting facilitate rapid detection of and response to security incidents. This timely response minimizes the impact of breaches, reduces downtime, and helps organizations recover more quickly from security events. The ability to automate and accelerate incident response is crucial in mitigating the damage and operational disruptions caused by cyber threats (Nourani, 2021).

Business analytics also enhances effective risk management by providing detailed insights into various risk factors. By analyzing data related to asset value, threat landscapes, and existing controls, organizations can prioritize their security measures based on the potential impact and likelihood of different threats. This targeted approach ensures that resources are allocated efficiently, focusing on the most critical vulnerabilities and threats, and thereby optimizing the overall security posture. Another notable advantage is the improved visibility and monitoring capabilities offered by business analytics. Advanced analytics tools provide comprehensive views of network activity and system performance, which enhance visibility into potential security issues. Continuous monitoring through these tools enables organizations to detect and address anomalies promptly, ensuring a proactive stance on security management.

Data-driven decision-making is significantly supported by business analytics, as these tools offer actionable insights derived from extensive data analysis. This information empowers security teams to make informed decisions regarding security strategies, resource allocation, and policy adjustments. Data-driven approaches enhance the effectiveness of security measures and help align them with organizational goals and risk management priorities. Automated threat intelligence is a further benefit of using business analytics in cybersecurity. By integrating threat intelligence feeds with analytics tools, organizations can automate the detection of known threats and vulnerabilities. This integration streamlines the process of identifying and addressing potential risks, reducing the manual effort required to keep up with the constantly evolving threat landscape.

Scalability and flexibility are additional advantages provided by modern business analytics solutions, particularly those that are cloud-based. These solutions allow organizations to handle large volumes of data efficiently and adapt to growing data needs as their operations expand. The ability to scale resources and manage data dynamically supports the effective analysis of complex and voluminous security data. Improved compliance and reporting are also facilitated by business analytics. Analytics tools generate detailed reports and dashboards that assist organizations in meeting regulatory requirements and internal security policies. These reports provide valuable insights into security performance and compliance status, ensuring better oversight and documentation of security practices. Also, behavioral analysis is an important aspect of business analytics in cybersecurity. By monitoring user and entity behavior, analytics tools can identify deviations from normal patterns that may suggest insider threats or compromised accounts. This capability enhances the ability to detect and respond to potential threats originating from within the organization (Greasley, 2019).

Table 3 contains the advantages of using business analytics in cybersecurity analytics within Industry 4.0 conditions, along with descriptions for each advantage. This table highlights the key advantages of leveraging business analytics in cybersecurity analytics, demonstrating how these tools enhance threat detection, response, and overall security management.

Table 3.
The advantages of using business analytics in cybersecurity analytics

Advantage	Description
Enhanced Threat Detection	Business analytics utilize advanced algorithms and machine learning to identify patterns and anomalies in vast amounts of data, improving the accuracy and speed of detecting potential security threats.
Predictive Capabilities	By analyzing historical data and trends, business analytics can forecast potential future threats and vulnerabilities, allowing organizations to implement preventive measures before incidents occur.
Improved Incident Response	Real-time data analysis and automated alerting help cybersecurity teams respond quickly to threats, reducing the impact of incidents and minimizing downtime.
Effective Risk Management	Business analytics provide detailed insights into risk factors, helping organizations prioritize security measures based on the potential impact and likelihood of various threats.
Enhanced Visibility and Monitoring	Advanced analytics offer comprehensive views of network activity and system performance, enabling better visibility into potential security issues and facilitating continuous monitoring.
Data-Driven Decision Making	Analytics tools provide actionable insights based on data, supporting informed decision-making for security strategies and resource allocation.
Automated Threat Intelligence	Integration of threat intelligence feeds with business analytics helps automate the detection of known threats and vulnerabilities, streamlining the identification of potential risks.
Scalability and Flexibility	Business analytics solutions, particularly cloud-based ones, offer scalability and flexibility, allowing organizations to manage and analyze large volumes of data efficiently as their needs grow.
Improved Compliance and Reporting	Analytics tools help generate detailed reports and dashboards that facilitate compliance with regulatory requirements and internal security policies, ensuring better oversight and documentation.
Behavioral Analysis	Business analytics enable the monitoring of user and entity behavior, identifying deviations from normal patterns that may indicate insider threats or compromised accounts.

Source: (Adel, 2022; Akundi et al., 2022; Olsen, 2023; Aslam, et al., 2020; Bakir, Dahlan, 2022; Cillo et al., 2022; Ghibakholl et al., 2022, Javaid, Haleem, 2020; Javaid et al., 2020; Cam et al., 2021; Charles et al., 2023; Greasley, 2019; Hurwitz et al., 2015; Nourani, 2021; Peter et al., 2023).

Table 4 contains the problems of using business analytics in cybersecurity analytics within Industry 4.0 conditions, along with descriptions for each advantage. This table highlights some of the common problems associated with the use of business analytics in cybersecurity, illustrating the challenges that organizations might face in leveraging these tools effectively.

Table 4.
The problems of using business analytics in cybersecurity analytics

Problem	Description
Data Overload	The sheer volume of data generated by cybersecurity systems can be overwhelming, making it challenging to identify and focus on relevant information.
False Positives	Analytics systems may generate false positives, flagging benign activities as threats, which can lead to unnecessary alerts and wasted resources.
Integration Challenges	Integrating business analytics tools with existing cybersecurity infrastructure and diverse data sources can be complex and may require significant customization.
Skill Gaps	Effective use of business analytics in cybersecurity requires specialized skills and knowledge, which may not be readily available within an organization.
Data Privacy Concerns	Analyzing large volumes of sensitive data raises concerns about data privacy and compliance with regulations, requiring stringent data protection measures.
High Costs	Implementing and maintaining advanced analytics solutions can be expensive, including costs for software, hardware, and skilled personnel.
Complexity of Analysis	The complexity of advanced analytics models can make it difficult to interpret results and take actionable steps, potentially leading to misinformed decisions.
Scalability Issues	As organizations grow, scaling analytics solutions to handle increasing volumes of data and more complex security environments can be challenging.
Dependence on Quality Data	Business analytics are highly dependent on the quality and accuracy of the data being analyzed. Poor data quality can lead to inaccurate or misleading results.
Over-Reliance on Automation	Excessive reliance on automated analytics tools might lead to overlooking contextual factors and nuanced threats that require human intervention and judgment.

Source: (Adel, 2022; Akundi et al., 2022; Olsen, 2023; Aslam, et al., 2020; Bakir, Dahlan, 2022; Cillo et al., 2022; Ghibakholl et al., 2022, Javaid, Haleem, 2020; Javaid et al., 2020; Cam et al., 2021; Charles et al., 2023; Greasley, 2019; Hurwitz et al., 2015; Nourani, 2021; Peter et al., 2023).

5. Conclusion

The integration of business analytics into cybersecurity practices within the context of Industry 4.0 represents a transformative advancement in protecting organizational assets from the evolving landscape of cyber threats. As industrial environments become increasingly complex and interconnected, the traditional security paradigms that focus solely on perimeter defenses are no longer sufficient. Instead, modern cybersecurity strategies must leverage sophisticated analytics to effectively manage and mitigate risks associated with this new era of digital transformation.

The application of business analytics in cybersecurity analytics offers significant benefits, including enhanced threat detection through advanced machine learning algorithms, predictive capabilities that allow organizations to anticipate and prepare for future threats, and improved incident response through real-time monitoring and automated alerts. These capabilities collectively contribute to a more proactive and efficient approach to cybersecurity, enabling organizations to not only detect and respond to incidents more swiftly but also to make informed decisions based on comprehensive risk assessments and performance measurements. However, the use of business analytics in cybersecurity is not without its challenges. Issues such as data overload, false positives, integration difficulties, and the need for specialized skills can complicate the effective implementation of analytics solutions. Additionally, concerns about data privacy, high costs, and the complexity of analysis must be addressed to ensure that the benefits of analytics outweigh the potential drawbacks.

As organizations continue to adapt to the demands of Industry 4.0, it is essential to approach business analytics in cybersecurity with a balanced perspective, recognizing both its transformative potential and its inherent limitations. By addressing these challenges and leveraging the strengths of analytics, organizations can enhance their security posture, optimize resource allocation, and improve their overall resilience against cyber threats. The ongoing evolution of business analytics technologies and practices will undoubtedly play a critical role in shaping the future of cybersecurity, making it imperative for organizations to stay informed and agile in their approach to digital security.

References

1. Adel, A. (2022). Future of industry 5.0 in society: human-centric solutions, challenges and prospective research areas. *Journal of Cloud Computing, 11(1),* 40.
2. Akundi, A., Euresti, D., Luna, S., Ankobiah, W., Lopes, A., Edinbarough, I. (2022). State of Industry 5.0-Analysis and Identification of Current Research Trends. *Applied System Innovation, 5(1),* DOI: 10.3390/asi5010027.
3. Aslam, F., Wang, A.M., Li, M.Z., Rehman, K.U. (2020). Innovation in the Era of IoT and Industry 5.0: Absolute Innovation Management (AIM) Framework. *Information, 11(2),* doi:10.3390/info11020124
4. Bakir, A., Dahlan, M. (2022). Higher education leadership and curricular design in industry 5.0 environment: a cursory glance. *Development and Learning in Organizations*.
5. Cam, J.D., Cochran, J.J., Ohlmann, M.J.F. (2021). *Business analytics: descriptive, predictive, prescriptive* Boston: Cengage.
6. Charles, V., Garg, P., Gupta, N., Agrawal, M. (2023). *Data Analytics and Business Intelligence: Computational Frameworks, Practices, and Applications*. New York: CRS Press.
7. Cillo, V., Gregori, G.L., Daniele, L.M., Caputo, F., Bitbol-Saba, N. (2022). Rethinking companies' culture through knowledge management lens during Industry 5.0 transition. *Journal of Knowledge Management, 26(10),* 2485-2498.

8. Dameri, R.P. (2016). Smart City and ICT. Shaping Urban Space for Better Quality of Life. In: *Information and Communication Technologies in Organizations and Society*. Cham, Switzerland: Springer International Publishing.
9. Di Marino, C., Rega, A., Vitolo, F., Patalano, S. (2023). Enhancing Human-Robot Collaboration in the Industry 5.0 Context: Workplace Layout Prototyping. *Lecture Notes in Mechanical Engineering,* 454-465.
10. Dutta, J., Roy, S., Chowdhury, C. (2019). Unified framework for IoT and smartphone based different smart city related applications. *Microsystem Technologies, 25(1),* 83-96.
11. Gajdzik, B., Jaciow, M., Wolniak, R., Wolny, R., Grebski, W. (2024). Diagnosis of the development of energy cooperatives in Poland - a case study of a renewable energy cooperative in the upper Silesian region. *Energies, 17(3),* 1-27, 647.
12. Gajdzik, B., Bartuś, K, Jaciow, M., Wolniak, R., Wolny, R., Grebski, W.W. (2024). Evolution of Polish E-Consumers' Environmental Awareness and Purchasing Behavior over Ten Years. *Sustainability, 16(11),* 4686.
13. Gajdzik, B., Jaciow, M., Wolniak, R. (2024). Gastronomic curiosity and consumer behavior: the impact of television culinary programs on choices of food services. *Foods, 13(1),* 1-16, 115.
14. Gajdzik, B., Siwiec, D., Wolniak, R., Pacana, A. (2024). Approaching open innovation in customization frameworks for product prototypes with emphasis on quality and life cycle assessment (QLCA). *Journal of Open Innovation: Technology, Market, and Complexity, 10(2),* 100268.
15. Gajdzik, B., Wolniak, R. (2021a). Digitalisation and innovation in the steel industry in Poland - selected tools of ICT in an analysis of statistical data and a case study. *Energies, 14(11),* 1-25.
16. Gajdzik, B., Wolniak, R. (2021b). Influence of the COVID-19 crisis on steel production in Poland compared to the financial crisis of 2009 and to boom periods in the market. *Resources, 10(1),* 1-17.
17. Gajdzik, B., Wolniak, R. (2021c). Transitioning of steel producers to the steelworks 4.0 - literature review with case studies. *Energies*, *14(14),* 1-22.
18. Gajdzik, B., Wolniak, R. (2022). Smart Production Workers in Terms of Creativity and Innovation: The Implication for Open Innovation. *Journal of Open Innovations: Technology, Market and Complexity, 8(1),* 68.
19. Gajdzik, B., Wolniak, R. (2022a). Framework for R&D&I Activities in the Steel Industry in Popularizing the Idea of Industry 4.0. *Journal of Open Innovation: Technology, Market, and Complexity, 8(3),* 133.
20. Gajdzik, B., Wolniak, R. (2022b). Influence of Industry 4.0 Projects on Business Operations: literature and empirical pilot studies based on case studies in Poland. *Journal of Open Innovation: Technology, Market, and Complexity, 8(1),* 1-20.

21. Gajdzik, B., Wolniak, R. (2022c). Smart Production Workers in Terms of Creativity and Innovation: The Implication for Open Innovation. *Journal of Open Innovations: Technology, Market and Complexity, 8(1),* 68.
22. Gajdzik, B., Wolniak, R., Grebski, W. (2023a). Process of Transformation to Net Zero Steelmaking: Decarbonisation Scenarios Based on the Analysis of the Polish Steel Industry. *Energies, 16(8), 3384,* https://doi.org/10.3390/en16083384.
23. Gajdzik, B., Wolniak, R., Nagaj, R., Žuromskaitė-Nagaj, B., Grebski, W. (2024). The influence of the global energy crisis on energy efficiency: a comprehensive analysis. *Energies, 17(4),* 1-49, 947.
24. Gajdzik, B., Wolniak, R., Grebski, W. (2023b). Electricity and heat demand in steel industry technological processes in Industry 4.0 conditions. *Energies, 16(2),* 1-29.
25. Gajdzik, B., Wolniak, R., Grebski, W.(2022). An econometric model of the operation of the steel industry in Poland in the context of process heat and energy consumption. *Energies, 15(21),* 1-26, 7909.
26. Gajdzik, B., Wolniak, R., Grebski, W.W. (2024). Challenges of industrial systems in terms of the crucial role of humans in the Industry 5.0 environment. *Production Engineering Archives, 30(1),* 1-16.
27. Gajdzik, B., Wolniak, R., Nagaj, R., Grebski, W., Romanyshyn, T. (2023). Barriers to Renewable Energy Source (RES) Installations as Determinants of Energy Consumption in EU Countries. *Energies, 16(21),* 7364.
28. Gębczyńska, A., Wolniak, R. (2018). *Process management level in local government.* Philadelphia: CreativeSpace.
29. Ghibakholl, M., Iranmanesh, M., Mubarak, M.F., Mubarik, M., Rejeb, A., Nilashi, M. (2022). Identifying industry 5.0 contributions to sustainable development: A strategy roadmap for delivering sustainability values. *Sustainable Production and Consumption, 33,* 716-737.
30. Grabowska, S., Saniuk, S., Gajdzik, B. (2022). Industry 5.0: improving humanization and sustainability of Industry 4.0. *Scientometrics, 127(6),* 3117-3144, https://doi.org/10.1007/s11192-022-04370-1.
31. Grabowska, S., Grebski, M., Grebski, W., Saniuk, S., Wolniak, R. (2021). *Inżynier w gospodarce 4.0.* Toruń: Towarzystwo Naukowe Organizacji i Kierownictwa – Stowarzyszenie Wyższej Użyteczności "Dom Organizatora".
32. Grabowska, S., Grebski, M., Grebski, W., Wolniak, R. (2019). *Introduction to engineering concepts from a creativity and innovativeness perspective.* New York: KDP Publishing.
33. Grabowska, S., Grebski, M., Grebski, W., Wolniak, R. (2020). *Inżynier – zawód przyszłości. Umiejętności i kompetencje inżynierskie w erze Przemysłu 4.0.* Warszawa: CeDeWu.
34. Greasley, A. (2019). *Simulating Business Processes for Descriptive, Predictive, and Prescriptive Analytics.* Boston: deGruyter.

35. Hąbek, P., Wolniak, R. (2013). Analysis of approaches to CSR reporting in selected European Union countries. *International Journal of Economics and Research*, *4(6),* 79-95.
36. Hąbek, P., Wolniak, R. (2016). Assessing the quality of corporate social responsibility reports: the case of reporting practices in selected European Union member states. *Quality & Quantity*, *50(1),* 339-420.
37. Hąbek, P., Wolniak, R. (2016). Factors influencing the development of CSR reporting practices: experts' versus preparers' points of view. *Engineering Economy*, *26(5),* 560-570.
38. Hąbek, P., Wolniak, R. (2016). Relationship between management practices and quality of CSR reports. *Procedia – Social and Behavioral Sciences*, *220*, 115-123.
39. Herdiansyah, H. (2023). Smart city based on community empowerment, social capital, and public trust in urban areas. *Glob. J. Environ. Sci. Manag.*, *9*, 113-128.
40. Hurwitz, J., Kaufman, M., Bowles, A. (2015). *Cognitive Computing and Big Data Analytics.* New York: Wiley.
41. Hys, K., Wolniak, R. (2018). Praktyki przedsiębiorstw przemysłu chemicznego w Polsce w zakresie CSR. *Przemysł Chemiczny*, *9*, 1000-1002.
42. Javaid, M., Haleem, A. (2020). Critical Components of Industry 5.0 Towards a Successful Adoption in the Field of Manufacturing. *Journal of Industrial Integration and Management-Innovation and Entrepreneurship*, *5(2),* 327-348, doi: 10.1142/ S2424862220500141.
43. Javaid, M., Haleem, A., Singh, R.P., Haq, M.I.U., Raina, A., Suman, R. (2020). Industry 5.0: Potential Applications in COVID-19. *Journal of Industrial Integration and Management-Innovation and Entrepreneurship*, *5(4),* 507-530, doi: 10.1142/ S2424862220500220.
44. Jonek-Kowalska, I., Wolniak, R. (2021a). Economic opportunities for creating smart cities in Poland. Does wealth matter? *Cities*, *114*, 1-6.
45. Jonek-Kowalska, I., Wolniak, R. (2021b). The influence of local economic conditions on start-ups and local open innovation system. *Journal of Open Innovations: Technology, Market and Complexity*, *7(2),* 1-19.
46. Jonek-Kowalska, I., Wolniak, R. (2022). Sharing economies' initiatives in municipal authorities' perspective: research evidence from Poland in the context of smart cities' development. *Sustainability*, *14(4),* 1-23.
47. Jonek-Kowalska, I., Wolniak, R. (2023). *Towards sustainability and a better quality of life?* London: Routledge.
48. Kordel, P., Wolniak, R. (2021). Technology entrepreneurship and the performance of enterprises in the conditions of Covid-19 pandemic: the fuzzy set analysis of waste to energy enterprises in Poland. *Energies*, *14(13),* 1-22.
49. Kwiotkowska, A., Gajdzik, B., Wolniak, R., Vveinhardt, J., Gębczyńska, M. (2021). Leadership competencies in making Industry 4.0 effective: the case of Polish heat and power industry. *Energies*, *14(14),* 1-22.

50. Kwiotkowska, A., Wolniak, R., Gajdzik, B., Gębczyńska, M. (2022). Configurational paths of leadership competency shortages and 4.0 leadership effectiveness: an fs/QCA study. *Sustainability, 14(5),* 1-21.
51. Michalak, A., Wolniak, R. (2023). The innovativeness of the country and the renewables and non-renewables in the energy mix on the example of European Union. *Journal of Open Innovation: Technology, Market, and Complexity, 9(2),* https://doi.org/10.1016/j.joitmc. 2023.100061.
52. Nagaj, R., Gajdzik, B., Wolniak, R., Grebski, W. (2024). The impact of deep decarbonization policy on the level of greenhouse gas emissions in the European Union. *Energies, 17(5),* 1-23, 1245.
53. Nourani, C.F. (2021). *Artificial Intelligence and Computing Logic: Cognitive Technology for AI Business Analytics (Innovation Management and Computing).* New York: CRC Press.
54. Olkiewicz, M., Olkiewicz, A., Wolniak, R., Wyszomirski, A. (2021). Effects of pro-ecological investments on an example of the heating industry - case study. *Energies, 14(18),* 1-24, 5959.
55. Olsen, C. (2023). Toward a Digital Sustainability Reporting Framework in Organizations in the Industry 5.0 Era: An Accounting Perspective. *Lecture Notes in Networks and Systems, 557,* 463-473.
56. Orzeł, B., Wolniak, R. (2021). Clusters of elements for quality assurance of health worker protection measures in times of COVID-19 pandemic. *Administrative Science, 11(2),* 1-14, 46.
57. Orzeł, B., Wolniak, R. (2022). Digitization in the design and construction industry - remote work in the context of sustainability: a study from Poland. *Sustainability, 14(3),* 1-25.
58. Peter, G.S., Amit, C.B., Deokar, V., Patel, N.R. (2023). *Machine Learning for Business Analytics: Concepts, Techniques and Applications in RapidMiner.* New York: Wiley.
59. Ponomarenko, T.V., Wolniak, R., Marinina, O.A. (2016). Corporate Social responsibility in coal industry (Practices of russian and european companies). *Journal of Mining Institute, 222,* 882-891.
60. Rosak-Szyrocka, J., Żywiołek J., Wolniak, R. (2023). Main reasons for religious tourism - from a quantitative analysis to a model. *International Journal for Quality Research, 1(17),* 109-120.
61. Scappini, A. (2016). *80 Fundamental Models for Business Analysts: Descriptive, Predictive, and Prescriptive Analytics Models with Ready-to-Use Excel Templates.* New York: Create Space.
62. Stawiarska, E., Szwajca, D., Matusek, M., Wolniak, R. (2020). *Wdrażanie rozwiązań przemysłu 4.0 w wybranych funkcjonalnych obszarach zarządzania przedsiębiorstw branży motoryzacyjnej: próba diagnozy.* Warszawa: CeDeWu.

63. Stawiarska, E., Szwajca, D., Matusek, M., Wolniak, R. (2021). Diagnosis of the maturity level of implementing Industry 4.0 solutions in selected functional areas of management of automotive companies in Poland. *Sustainability, 13(9),* 1-38.
64. Stecuła, K., Wolniak, R. (2022). Advantages and Disadvantages of E-Learning Innovations during COVID-19 Pandemic in Higher Education in Poland. *Journal of Open Innovation: Technology, Market, and Complexity, 8(3),* 159.
65. Stecuła, K., Wolniak, R. (2022). Influence of COVID-19 Pandemic on Dissemination of Innovative E-Learning Tools in Higher Education in Poland. *Journal of Open Innovations: Technology, Market and Complexity, 8(1),* 89.
66. Wolniak, R., Skotnicka-Zasadzień, B. (2014). The use of value stream mapping to introduction of organizational innovation in industry. *Metalurgija*, *53(4)*, 709-713.
67. Wolniak, R. (2011). *Parametryzacja kryteriów oceny poziomu dojrzałości systemu zarządzania jakością.* Gliwice: Wydawnictwo Politechniki Śląskiej.
68. Wolniak, R. (2013). Projakościowa typologia kultur organizacyjnych. *Przegląd Organizacji*, *3,* 13-17.
69. Wolniak, R. (2014). Korzyści doskonalenia systemów zarządzania jakością opartych o wymagania normy ISO 9001:2009. *Problemy Jakości*, *3,* 20-25.
70. Wolniak, R. (2016a). Kulturowe aspekty zarządzania jakością. *Etyka biznesu i zrównoważony rozwój. Interdyscyplinarne studia teoretyczno-empiryczne*, *1,* 109-122.
71. Wolniak, R. (2016b). *Metoda QFD w zarządzaniu jakością. Teoria i praktyka*. Gliwice: Wydawnictwo Politechniki Śląskiej.
72. Wolniak, R. (2016c). Relations between corporate social responsibility reporting and the concept of greenwashing. *Zeszyty Naukowe Politechniki Śląskiej. Seria Organizacji i Zarządzanie, 87,* 443-453.
73. Wolniak, R. (2016d). The role of QFD method in creating innovation. *Systemy Wspomagania Inżynierii Produkcji, 3*, 127-134.
74. Wolniak, R. (2017a). Analiza relacji pomiędzy wskaźnikiem innowacyjności a nasyceniem kraju certyfikatami ISO 9001, ISO 14001 oraz ISO/TS 16949. *Kwartalnik Organizacja i Kierowanie*, *2*, 139-150.
75. Wolniak, R. (2017b). Analiza wskaźników nasycenia certyfikatami ISO 9001, ISO 14001 oraz ISO/TS 16949 oraz zależności pomiędzy nimi. *Zeszyty Naukowe Politechniki Śląskiej. Seria Organizacji i Zarządzanie*, *108*, 421-430.
76. Wolniak, R. (2017c). The Corporate Social Responsibility practices in mining sector in Spain and in Poland – similarities and differences. *Zeszyty Naukowe Politechniki Śląskiej. Seria Organizacji i Zarządzanie*, *111*, 111-120.
77. Wolniak, R. (2017d). The Design Thinking method and its stages. *Systemy Wspomagania Inżynierii Produkcji, 6*, 247-255.
78. Wolniak, R. (2021). Performance evaluation in ISO 9001:2015. *Silesian University of Technology Scientific Papers. Organization and Management Series*, *151*, 725-734.

79. Wolniak, R. (2022a). Innovations in Industry 4.0 conditions. *Silesian University of Technology Scientific Papers. Organization and Management Series, 169,* 725-741.
80. Wolniak, R. (2022b). Functioning of real-time analytics in business. *Silesian University of Technology Scientific Papers. Organization and Management Series, 172,* 659-677.
81. Wolniak, R. (2023a). Deskryptywna analiza danych. *Zarządzanie i Jakość, 5(2),* 282-290.
82. Wolniak, R. (2023b). Smart biking w smart city. *Zarządzanie i Jakość, 5(2),* 313-328.
83. Wolniak, R. (2023c). Analiza w czasie rzeczywistym. *Zarządzanie i Jakość, 5(2),* 291-312.
84. Wolniak, R. (2023d). Smart mobility jako element koncepcji smart city. *Zarządzanie i Jakość, 5(2),* 282-290.
85. Wolniak, R., Gajdzik, B., Grebski, M., Danel, R., Grebski, W.W. (2024). Business Models Used in Smart Cities—Theoretical Approach with Examples of Smart Cities. *Smart Cities, 7(4),* 1626-1669.
86. Wolniak, R., Jonek-Kowalska, I. (2021a). The level of the quality of life in the city and its monitoring. *Innovation (Abingdon*), *34(3),* 376-398.
87. Wolniak, R., Jonek-Kowalska, I. (2021c). The quality of service to residents by public administration on the example of municipal offices in Poland. *Administration Management Public*, *37*, 132-150.
88. Wolniak, R., Jonek-Kowalska, I. (2022). The creative services sector in Polish cities. *Journal of Open Innovation: Technology, Market, and Complexity*, *8(1),* 1-23.
89. Wolniak, R., Saniuk, S., Grabowska, S., Gajdzik, B. (2020). Identification of energy efficiency trends in the context of the development of Industry 4.0 using the Polish steel sector as an example. *Energies*, *13(11),* 1-16.
90. Wolniak, R., Skotnicka, B. (2011).: *Metody i narzędzia zarządzania jakością – Teoria i praktyka, cz. 1*. Gliwice: Wydawnictwo Naukowe Politechniki Śląskiej.
91. Wolniak, R., Skotnicka-Zasadzień, B. (2008). *Wybrane metody badania satysfakcji klienta i oceny dostawców w organizacjach.* Gliwice: Wydawnictwo Politechniki Śląskiej.
92. Wolniak, R., Skotnicka-Zasadzień, B. (2010). *Zarządzanie jakością dla inżynierów.* Gliwice: Wydawnictwo Politechniki Śląskiej.
93. Wolniak, R., Skotnicka-Zasadzień, B. (2018). Developing a model of factors influencing the quality of service for disabled customers in the condition s of sustainable development, illustrated by an example of the Silesian Voivodeship public administration. *Sustainability, 7, 1*-17.
94. Wolniak, R., Skotnicka-Zasadzień, B. (2022). Development of photovoltaic energy in EU countries as an alternative to fossil fuels. *Energies*, *15(2),* 1-23.
95. Wolniak, R., Skotnicka-Zasadzień, B. (2023). Development of Wind Energy in EU Countries as an Alternative Resource to Fossil Fuels in the Years 2016-2022. *Resources, 12(8),* 96.

96. Wolniak, R., Skotnicka-Zasadzień, B., Zasadzień, M. (2019). Problems of the functioning of e-administration in the Silesian region of Poland from the perspective of a person with disabilities. *Transylvanian Review of Public Administration*, *57E,* 137-155.
97. Wolniak, R., Stecuła, K. (2024). Artificial Intelligence in Smart Cities—Applications, Barriers, and Future Directions: A Review. *Smart Cities*, *7(3),* 1346-1389.
98. Wolniak, R., Sułkowski, M. (2015). Motywy wdrażanie certyfikowanych Systemów Zarządzania Jakością. *Problemy Jakości, 9,* 4-9.
99. Wolniak, R., Sułkowski, M. (2016). The reasons for the implementation of quality management systems in organizations. *Zeszyty Naukowe Politechniki Śląskiej. Seria Organizacji i Zarządzanie*, *92*, 443-455.
100. Wolniak, R., Wyszomirski, A., Olkiewicz, M., Olkiewicz, A. (2021). Environmental corporate social responsibility activities in heating industry - case study. *Energies*, *14(7),* 1-19, 1930.