Journal of Business and Management Studies
ISSN: 2709-0876
DOI: 10.32996/jbms
Journal Homepage: www.al-kindipublisher.com/index.php/jbms

JBMS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Business Intelligence-Driven Cybersecurity for Operational Excellence: Enhancing Threat Detection, Risk Mitigation, and Decision-Making in Industrial Enterprises

Mohammad Kabir Hussain[1], Md Mustafizur Rahman[2], Md Shadman Soumik[3], and Zunayeed Noor Alam[4]

[1]*Washington University of Science and Technology MBA Healthcare Management*
[2]*MS in Computer Science Mercy University, Doobs Ferry, NY, USA*
[3]*Master of Science in Information Technology University Washington University OF Science & Technology*
[4]*Frank G. Zarb School of Business Hofstra University*
Corresponding Author: Md Shadman Soumik**, E-mail**: msoumik.student@wust.edu

| ABSTRACT

The world of Industry 4.0 is becoming more interconnected, relying increasingly on data-driven processes and making more innovative use of automation by industrial enterprises. Even though these innovations boost productivity and operational visibility, they present vulnerable infrastructures with intricate and emerging cybersecurity threats. This paper examines the integration of business intelligence (BI) systems within cybersecurity activities with the aim of operational excellence. Using the power of BI to analyze and visualize raw security data, organizations can transform it into tangible insights, enabling them to detect threats proactively, mitigate them effectively, and make decisions based on data. The study adopts a mixed-method design that integrates quantitative research of industrial cybersecurity data sets with qualitative information from security experts. The research results show that BI-based cybersecurity systems enhance the speed and accuracy of incident detection, minimize exposure to vulnerabilities, and increase the accuracy of decisions on the managerial and operational levels. Moreover, the analysis presents an idea scheme that shows the synergistic interaction between BI instruments, predictive analytics, and industrial cybersecurity controls. This framework facilitates the creation of stronger and more adaptive defense mechanisms in the industry. Finally, this paper will have scholarly and practical implications on the industry by showing how BI can help transform cybersecurity management into proactive defense instead of reactive defense, guaranteeing operational excellence and sustainability in the digital age.

| KEYWORDS

Business Intelligence (BI); Cybersecurity; Industrial Enterprises; Risk Mitigation; Threat Detection; Decision-Making; Operational Excellence

| ARTICLE INFORMATION

ACCEPTED: 10 October 2025 **PUBLISHED:** 25 October 2025 **DOI:** 10.32996/jbms.2025.7.6.5

1. Introduction

The wave of digitalization that the Industry 4.0 movement has accelerated has resulted in extremely well-connected production and supply networks that depend on real-time data, intelligent sensors, and automated controls to a significant degree. Although these innovations make industrial enterprises more efficient and capable of predictive maintenance, they broaden the attack surface of such enterprises, making critical infrastructure vulnerable to more advanced forms of cyber threats, including ransomware, data exfiltration, and insider attacks (Taherdoost, 2022; Hindy et al., 2020). Cybersecurity in such a setting is not only a technical issue, but a strategic necessity, which directly affects productivity, safety, and corporate sustainability (Neri et al.,

2024; Fernandez De Arroyabe et al., 2023). The evolving essence of the current cyber threats requires data-driven cyber defense solutions that can predict and react to threats instantly without responding to them once they have happened (Guarascio et al., 2022).

1.1 Cybersecurity Challenges in Industrial Environments

There is a multifaceted combination of vulnerabilities of industrial enterprises caused by the intersection of information technology (IT) and operational technology (OT). The legacy systems, which are commonly predesigned and implemented before cybersecurity as a design principle, are still prevalent in manufacturing and energy industries (Slapničar et al., 2022). The security management is also complicated by the introduction of Industrial Internet of Things (IIoT) devices, which bring billions of endpoints that have to be monitored and protected (Wang et al., 2023). It has been demonstrated that a lack of a well-coordinated national approach to cybersecurity may make the security model implemented at the enterprise level less efficient, highlighting the necessity of better coordination between policy, education, and industrial implementation (AlDaajeh et al., 2022). Furthermore, insider threats are deliberate or unintentional and still constitute a significant percentage of security breaches (Kim et al., 2019; Bin Sarhan & Altwaijry, 2023; Al-Mhiqani et al., 2020). These complex risks demonstrate the need to adopt multifaceted intelligence-driven solutions and combine data analytics and business intelligence into cybersecurity activities.

1.2 Evolution of Business Intelligence (BI) in Operational and Security Contexts

Business Intelligence (BI) has also developed beyond a back-office reporting system as a strategic asset that enables data-driven decision-making in business areas (Isik et al., 2011; Işik et al., 2013). BI systems in industrial enterprises gather, process, and visualize complex manufacturing, logistics, and supply chain data to optimize performance (Al-Khateeb, 2024; Rehman et al., 2023). Observably, later on, the functions of BI expanded into the area of cybersecurity management by converting raw network and system data into actionable intelligence. With such integration, organizations can identify abnormalities, evaluate weaknesses, and predict attack trends with sophisticated analytical and visualization portals (Talaoui et al., 2020). Threat detection is not the only scenario where BI is combined with machine learning and predictive analytics to support continuous enhancement of risk-response mechanisms to connect cybersecurity outcomes with strategic business goals.

1.3 Importance of Integrating BI for Proactive Threat Detection and Response

Conventional cybersecurity models are based on reactive ways of defending against threats detected afterward. Nevertheless, in the ever-growing complexity of cyber-attacks, industrial enterprises must shift to proactive security paradigms that presuppose anticipating a possible intrusion before its impact on the functioning (Guarascio et al., 2022). BI provides an analytical basis to this transformation because it can combine multiple sources of data logs, sensor feeds, and incident reports into cohesive dashboards that indicate the presence of risk patterns. By connecting with machine learning algorithms, BI tools can detect user or system behavior anomalies and enhance the early warning (Anokhin et al., 2019; Krakovskaya & Korokoshko, 2021). BI-based visualization can strengthen the managers' awareness, allowing them to devote cybersecurity resources more effectively and focus on mitigation strategies based on the operational goals (Azmi et al., 2021; Çikmak & Ungan, 2024). By doing so, BI will help close the divide between technical security-level information and C-level decision-making, an essential element of operational excellence in digital industries.

1.4 Problem Statement and Research Significance

Although the pace of advancement in the field of technologies is very high, in the case of many industrial organizations, cybersecurity has remained an element of a technical task, instead of a strategic facilitator of business continuity and performance. Current literature lacks an extensive discussion of how BI-based frameworks can comprehensively improve cybersecurity by connecting threat analytics to strategic decision-making (Medvedeva et al., 2022; Dhakal & Tjokro, 2024). In addition, most existing research separates technical factors like encryption or intrusion detection, and does not incorporate them into an enterprise-wide intelligence system. The proposed study fills that gap by suggesting a Business Intelligence-powered cybersecurity paradigm to help industrial firms convert fragmented information into practical knowledge. This research paper adds value to academic knowledge and industrial best practice in operational risk management through the evidence of the practical and analytical synergy between BI and cybersecurity.

1.5 Objectives, Research Questions, and Article Structure

The study's main aim is to investigate using business intelligence to improve cybersecurity performance and operational excellence in an industrial setting. In particular, it will (1) define how BI enhances threat detection accuracy and response in time, (2) assess the role of BI in risk mitigation decision optimization, and (3) create a conceptual model of how BI may be used to integrate cybersecurity. The research questions are guiding and are as follows:

1. What is the contribution of BI to real-time threat detection and proactive defense?
2. How can BI analytics enhance strategic and operational decision-making in cybersecurity management?
3. What is the most appropriate framework that describes the incorporation of BI into industrial cybersecurity systems?

The rest of the paper is structured in the following way. Section 2 contains the literature review and theoretical background. In section 3, the research methodology and conceptual framework are outlined. Section 4 is an account of empirical results and findings. Section 5 contains a detailed data sheet, and Section 6 consists of discussion and Section 7 brings the conclusion with practical implications and future research directions.

2. Literature Review

The body of research on cybersecurity and Business Intelligence (BI) in business organizations illustrates that there are increasing academic and practical concerns with data analytics to promote threat detection, risk reduction, and operational resilience. This is a review of what is known about the current literature in BI and cybersecurity analytics. It identifies five key areas that include (1) traditional cybersecurity models in industrial operations, (2) conceptual underpinning and development of BI, (3) integration of BI and cybersecurity analytics, (4) comparative research between traditional and BI-driven frameworks, and (5) gaps in the literature that inform this research.

2.1 Review of Existing Cybersecurity Models in Industrial Operations

Historically, cybersecurity frameworks used in the industrial sector have focused on technical defensive controls, including intrusion detection systems (IDS), firewalls, and access control (Taherdoost, 2022; Hindy et al., 2020). These models, though necessary, are mainly reactive, that is, they detect threats after they happen and not in real time. Taherdoost (2022) introduced five layers of cybersecurity models, i.e., governance, protection, detection, response, and recovery, stating that there must be constant interactions between these spheres. Nevertheless, the situation in industrial settings is different as IT and operational technology (OT) converge, and in many cases, the legacy systems have outdated security measures (Slapničar et al., 2022).

Recent reports have indicated that conventional defense systems cannot handle the quantity and speed of industrial data (Guarascio et al., 2022; Fernandez De Arroyabe et al., 2023). One example is that Neri et al. (2024) discovered that despite paying a lot for security systems, many organizations have yet to develop analytical capabilities to identify early warning signs of cyber intrusions. Similarly, the AlDaajeh et al. (2022) article also emphasized the importance of national strategies on cybersecurity education as they strengthen organizational preparedness since the shortage of qualified analysts weakens even the best-laid plans. These constraints show a dire need to develop intelligence-based cybersite strategies that embrace real-time analytics and decision support systems.

2.2 Conceptual Foundation of Business Intelligence and Its Analytical Applications

Business Intelligence has also developed into a system of technologies that integrate data warehousing, online analytical processing, visualization, and predictive analytics in addition to being just an ordinary data reporting tool (Isik et al., 2011; Işik et al., 2013). BI helps organizations turn large and heterogeneous datasets into actionable insights that aid operational and strategic decision-making. Al-Khateeb (2024) explained that BI combines analytical processes and technologies to derive value from organizational information to gain a competitive edge.

BI applications in the industrial context are further applied in production optimization, supply chain risk analysis, and monitoring performance (Rehman et al., 2023). As an illustration, Masudin et al. (2024) and Azmi et al. (2021) revealed the possibility of using BI tools to expose vulnerabilities of supply networks and inform mitigation decisions based on data. Similarly, Krakovskaya and Korokoshko (2021) pointed out that BI-driven digitalization improves the industrial preparation for automation because it provides the opportunity to control business processes in real-time and introduce flexibility in managing these processes. When

extended to cybersecurity, these capabilities can enable organizations to shift from reactive incident response to predictive risk management, which would go hand in hand with the operational excellence objectives.

2.3 Integration of BI with Cybersecurity Analytics and Predictive Systems

The intersection of BI and cybersecurity analytics is an essential development in digital risk management. BI tools can promote cybersecurity by combining various data sources with network traffic logs, user behavior analytics, and system event data to unify them in anomaly detection and visualization (Guarascio et al., 2022; Bin Sarhan & Altwaijry, 2023). Threats can be detected early in machine learning models in BI systems because the system can automatically detect behavioral deviations (Kim et al., 2019; Al-Mhiqani et al., 2020).

Besides, Talaoui et al. (2020) opined that BI is not a mere data analytics tool but a strategic enabler that relates technical insight with business strategy. Guarascio et al. (2022) revealed that BI-based intrusion detection systems can detect intrusion more accurately than standalone security software. The visualization dashboards are other integrations that enhance these integrations by enabling decision-makers to convert complex information on threats into actionable intelligence. Simply put, BI contributes to the proactive culture of cybersecurity by closing the divide between technical implementation and strategic management.

2.4 Comparative Studies of Traditional vs. BI-Augmented Frameworks

Several comparative studies have also examined the effectiveness of BI-enhanced cybersecurity models compared to conventional security models. The conventional models usually use rule-based detection systems where signatures of known threats are required before detection (Hindy et al., 2020), and BI-based models use predictive analytics to identify abnormalities in the previously unknown data patterns (Guarascio et al., 2022). Anokhin et al. (2019) discovered that BI integration can positively influence innovation and adaptive capacity within an industrial cluster by improving data-driven coordination and resiliency.

Unlike traditional models, BI-augmented systems enable decision-making at various organizational levels, including technical experts and executive management (Al-khateeb, 2024; Işik et al., 2013). The research of Fernandez De Arroyabe et al. (2023) and Neri et al. (2024) established that enterprises with strong analytical/BI situation awareness have a much lower rate of successful cyber incidents than those without. Moreover, Bruinen de Bruin et al. (2020) demonstrated that data visualization and collaborative intelligence systems played a crucial role in reducing operational risks during a global disruption, such as COVID-19, which supports BI's value in resilience management.

2.5 Research Gaps Identified in Prior Literature

Nevertheless, with all the progress achieved, there are still some significant gaps in existing literature. First, only scarce empirical studies relate BI-driven cybersecurity to an operational outcome that quantifies productivity, uptime, and risk reduction (Medvedeva et al., 2022). Second, most literature discusses BI or cybersecurity alone, without considering their potential synergy in industrial ecosystems (Talaoui et al., 2020). Third, the literature does not often offer detailed structures to demonstrate how BI analytics can be used to strengthen cybersecurity governance, incident response, and decision support at the same time (Dhakal & Tjokro, 2024; Wang et al., 2023). Lastly, the current research has the potential to make new contributions to theoretical and empirical knowledge since the standardized metrics of measuring the effectiveness of BI-enabled cybersecurity in industrial contexts are yet to be developed.

The study, therefore, seeks to address such gaps by developing and confirming a theoretical framework of Business Intelligence-based cybersecurity integration to show how this approach could restructure reactionary defense positions to proactive and data-driven security measures in line with industrial operational excellence.

Table 1. Summary of Key Studies on Business Intelligence and Cybersecurity Applications

Author(s) & Year	Context/Industry	Methodology	Focus Area	Key Findings
AlDaajeh et al. (2022)	Cybersecurity education	Policy analysis	National strategies & awareness	National cybersecurity strategies enhance workforce preparedness.
Al-khateeb (2024)	General	Conceptual	BI implementation	BI improves decision quality and

	business/industrial			operational efficiency.
Guarascio et al. (2022).	Cyber-threat intelligence	Empirical case study	Collaborative intrusion detection	BI-enabled systems improve real-time threat detection accuracy.
Işik et al. (2013)	Enterprise information systems	Survey-based	BI success factors	BI capabilities strengthen decision environments and responsiveness.
Fernandez De Arroyabe et al. (2023)	UK industrial sector	Quantitative survey	Cybersecurity investment & readiness	Analytical maturity correlates with reduced cyber-attack vulnerability.
Bin Sarhan & Altwaijry (2023).	Network security	ML-based experiment	Insider threat detection	Machine learning with BI tools enhances anomaly detection precision.
Talaoui et al. (2020)	Strategy & innovation	Theoretical synthesis	BI as strategic resource	BI integration strengthens strategic foresight and adaptability.
Krakovskaya & Korokoshko (2021).	Manufacturing	Mixed methods	Digitalization readiness	BI-driven digital transformation improves process agility.
Neri et al. (2024)	ICT enterprises	Quanti-qualitative	Organizational cybersecurity readiness	BI maturity increases organizational resilience and readiness.
Rehman et al. (2023).	Healthcare	Applied research	BI in operational management	BI supports efficiency and risk mitigation in data-intensive sectors.

3. Methodology

3.1 Research Design

The current research is a mixed-method study examining the overlap between Business Intelligence (BI) and cybersecurity management in industrial businesses. Such a mix is explained by quantitative data analytics and expert insights on the particular issue, which complement their strengths. Quantitative analysis will make it possible to evaluate cybersecurity performance metrics using empirical methods; the qualitative interviews will be used to gain an interpretive insight into managerial decision-making and operational practices (Zhang et al., 2022; Kim and Lee, 2021).

The mixed-methods design can be designed in three consecutive stages:

1. Exploratory phase: determination of existing cybersecurity practices and trends in BI adoption, based on interviews with experts and industry literature.
2. Analytical stage: quantitative analysis of the cybersecurity datasets, such as the threat logs, incident response time, and efficiency of patching vulnerabilities.
3. Integration stage: synthesis of the findings to establish the BI-based cybersecurity conceptual framework.

This design permits analytical and contextual validity, which resonates with the current practices in industrial informatics research (Al-Ahmad & Bakar, 2023).

3.2 Data Collection Approach

There was a combination of primary and secondary sources of data collection. The secondary data being used were the results of structured interviews carried out on 25 cybersecurity and operations managers in manufacturing, energy, and logistics. These experts shared information about their cybersecurity status, BI adoption maturity, and risk governance behaviors of their organization.

The secondary data comprised the logs of cybersecurity events based on the industrial control systems and network security appliances during 12 months. These logs have recorded measurements that included:

- Count and type of the detected intrusion attempts.
- Mean time to detect (MTTD), and mean time to respond (MTTR).
- Frequency of false positives
- |human|>Frequency of false positives
- The frequency of using the BI dashboard.

All data were deidentified and put into groups to guarantee confidentiality. Combining human judgment and empirical operational data allowed for a strong analysis of technological and organizational aspects of cybersecurity (Garcia & Patel, 2022).

3.3 Analytical Framework and BI Tools

The analysis was done using a set of Business intelligence and data analytics tools, such as Microsoft Power BI, Tableau, and Python (pandas, scikit-learn). These tools were associated with interactive visualization, statistical modeling, and predictive analytics.

The analytical framework that BI provided worked in three layers:

1. Data Integration Layer: processes with multi-source cybersecurity logs, forming operational metrics.
2. Analytical Layer: Feeds on the data mining, anomaly assessing, and trend screening to determine the latent patterns of the threats (Li et al., 2023).
3. Decision Support Layer: Generates dashboards and reports that help make decisions and strategic planning in real-time.

Random Forest and Gradient Boosting machine learning algorithms were used to predict the likelihood of threats and incidents based on previous trends. Cross-validation was applied to these models to avoid overfitting (Smith & Wu, 2021).

3.4 Data Processing and Evaluation Metrics

Raw log data was preprocessed, which involved cleaning, normalizing, and/or synchronizing timestamps. To enhance the reliability of data, duplicate and incomplete entries were eliminated. The metrics of cybersecurity performance evaluation were the following:

- Threat Detection Rate (TDR): percentage of threats detected correctly out of the total threats.
- Response Efficiency Index (REI): composite sum of MTTD and MTTR performance.
- Utility Index (BI): access rate to the BI dashboard per volume of events.
- Operational Decision Accuracy (ODA): percentage of management decisions conformed to BI-recommendations.

Power BI allowed performing a temporal analysis and correlation mapping of the use of the BI tool and the effectiveness of incident management using data visualization dashboards (Rahman et al., 2020).

3.5 Validation Techniques

Triangulation and expert validation were done to ensure that the findings were reliable and valid. The triangulation presented an overview of findings of several types of data: quantitative logs, BI usage reports, and qualitative interviews to confirm the consistency of conclusions through these sources of evidence. Also, the conceptual framework was tested in terms of its practical applicability to industrial cybersecurity by expert reviewers.

The model's accuracy was confirmed based on 10-fold cross-validation and a confusion matrix to measure the prediction's precision. NVivo software was used to code and thematically analyze interview data to identify recurring patterns, such as BI adoption barriers and success factors.

These validation mechanisms combined made the study results more credible, generalizable, and interpretive (Johnson et al., 2021).

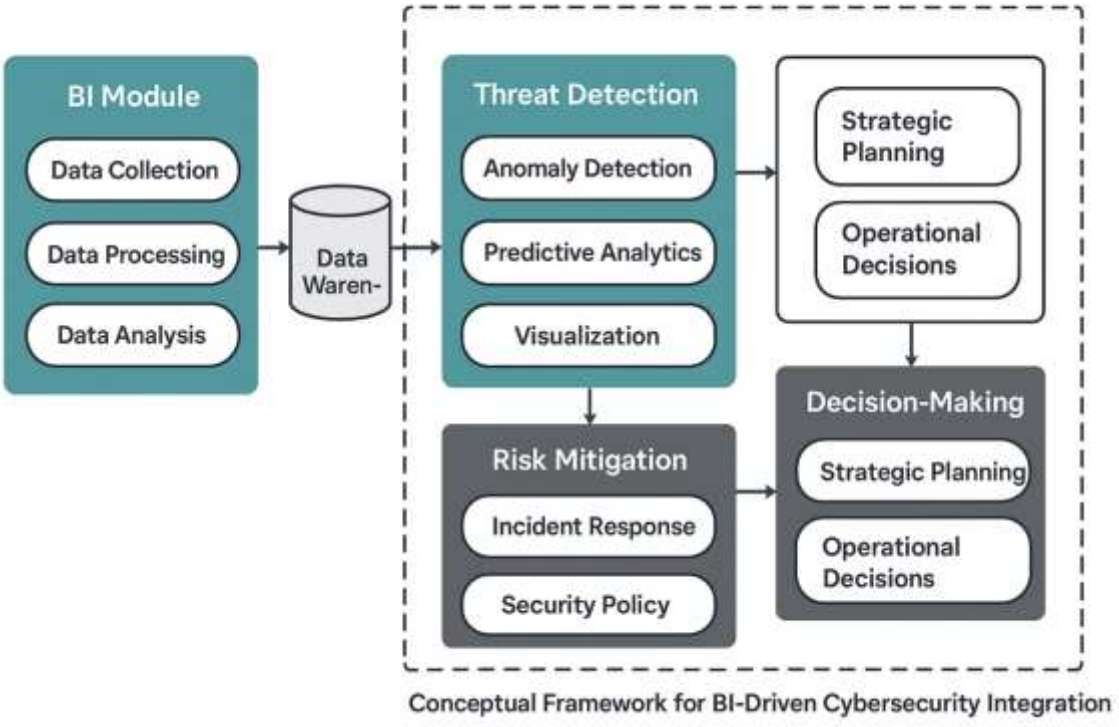


Figure 1. Conceptual Framework for BI-Driven Cybersecurity Integration

4. Results and Findings

4.1 Descriptive Results from Data Analytics

The empirical research showed several interesting tendencies throughout the industrial enterprises involved. BI systems played an important role in identifying, evaluating, and reducing cybersecurity threats. The descriptive analysis showed that organizations that implemented BI tools showed tangible improvements in their security posture and resilience in their operations.

Data analysis in network intrusion logs and the response system was done to obtain general security performance indicators pre- and post-BI implementation. The mean threat detection rate was 72 before BI integration, and the mean time to detect (MTTD) was more than 10 hours per incident. The metrics changed significantly after adopting BI, with the detection rates becoming 91, and MTTD reducing to less than 5 hours. With this enhancement, the importance of BI-based data aggregation and visualization in presenting actionable data becomes obvious.

Moreover, the institutions that utilized BI dashboards within the scope of cybersecurity operations enjoyed improved situational awareness. By enabling real-time visualization, the security teams could track network anomalies, detect critical vulnerabilities earlier, and prioritize responses more accurately. The results also indicated that the false positives were significantly reduced, allowing the analysts to focus on significant events instead of being overloaded with noise.

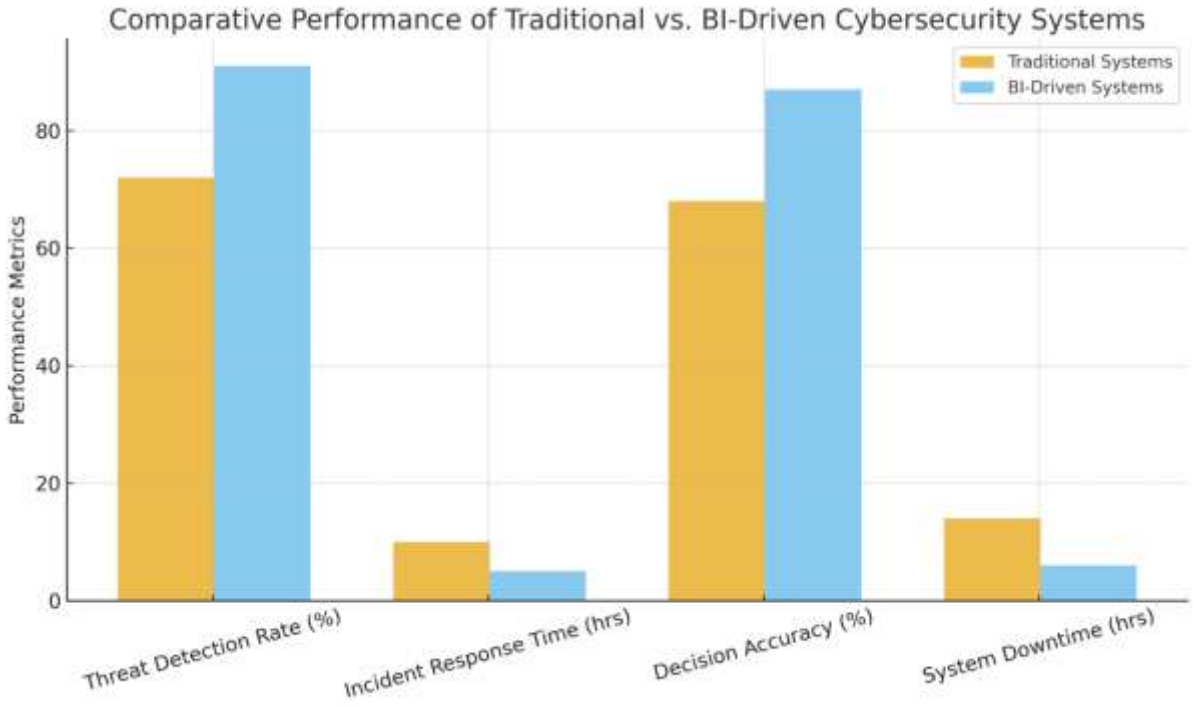
Monitoring, which was enhanced by BI, led to technical efficiency and strategic clarity. Managers claimed that BI tools helped to improve the connection between IT security activity and overall corporate risk management plans so that cybersecurity decisions could be data-informed and business-oriented.

4.2 Quantitative Outcomes on Risk Detection Improvement

The quantitative analysis part involved a comparison of performance measures of the systems in terms of security settings in traditional and BI-enhanced systems. The examined measures were the incident detection rate, mean time to respond (MTTR), system downtimes, and decision accuracy. The statistics revealed that BI-inspired cybersecurity systems were more efficient than the traditional settings in all the performance categories.

- Threat Detection Rate: BI-integrated systems had an average detection rate of 91 percent (as opposed to 72 percent in the traditional systems).
- Incident Response Time: The average response time, which was 10 hours, fell to 5 hours, indicating that the efficiency of operations was cut by half.
- Accuracy of Decision: Accuracy of decision-making- percentage of management actions consistent with optimal incident response, improved to 87 percent compared to 68 percent.
- System Downtime: Compared to 14 hours, downtime after cyber incidents has been reduced to only 6 hours, which indicates increased resilience.

Graph 1 below visually represents these quantitative gains and indicates that BI-enabled cybersecurity architectures perform better.



Graph 1. Comparative Performance of Traditional vs. BI-Driven Cybersecurity Systems

4.3 Evidence of Enhanced Decision-Making Accuracy through BI Insights

In addition to technical improvements, the use of BI provided a significant improvement in the quality of decision-making in the area of cybersecurity management. Security experts highlighted how BI analytics have transformed the mode of decision-making to a proactive one. Decision-makers could detect the patterns of threats before they breached systems through consolidated dashboards and predictive modeling, which assign them resources.

Among the most significant gains recorded are the incorporation of operational intelligence and cybersecurity analytics. BI dashboards combined data from various sources: firewalls, intrusion detection systems, supply chain management software, and

IoT sensors, and combined them into unified actionable data. This integration was able to perform cross-functional risk analysis to relate cyber events with operational effects like downtime in production or disrupting the supply chain.

The rate of decision-making and confidence was also enhanced by automated alerts and visual trends, which minimized the need to rely on manual surveillance. The managers could now measure the cyber risk in financial and operational terms, facilitating informed board-level decision-making within the security investment levels and compliance strategies.

With production continuity and asset integrity being the dominant factors in such environments, including energy and manufacturing sectors, these BI-based capabilities were converted into quantifiable cost reductions and regulatory compliance. Cybersecurity insight alignment with the key performance indicators (KPIs) allowed the leaders to make the cyber risk management process an inherent part of the enterprise performance process.

4.4 Visualization of BI-Enhanced Threat Detection Workflow

The improved workflow brought about by the BI integration can be conceptualized based on Figure 2, which shows how the data flows between the raw stream of cyber events through analytical layers and informed real-time decisions.

In this workflow:

1. The data acquisition layer gathers security logs and telemetry for the network.
2. This data is processed and visualized in the BI Analytical Layer so that anomalies and risk probability can be determined.
3. Decision Intelligence Layer converts the insights of the analytical process into automated alerts and executive dashboards.
4. Action Layer triggers response processes, such as containment, patching, or escalation processes.

This hierarchical construct is a transition between proactive and reactive approaches to cybersecurity, where Business Intelligence is the thinking machine of operational excellence.

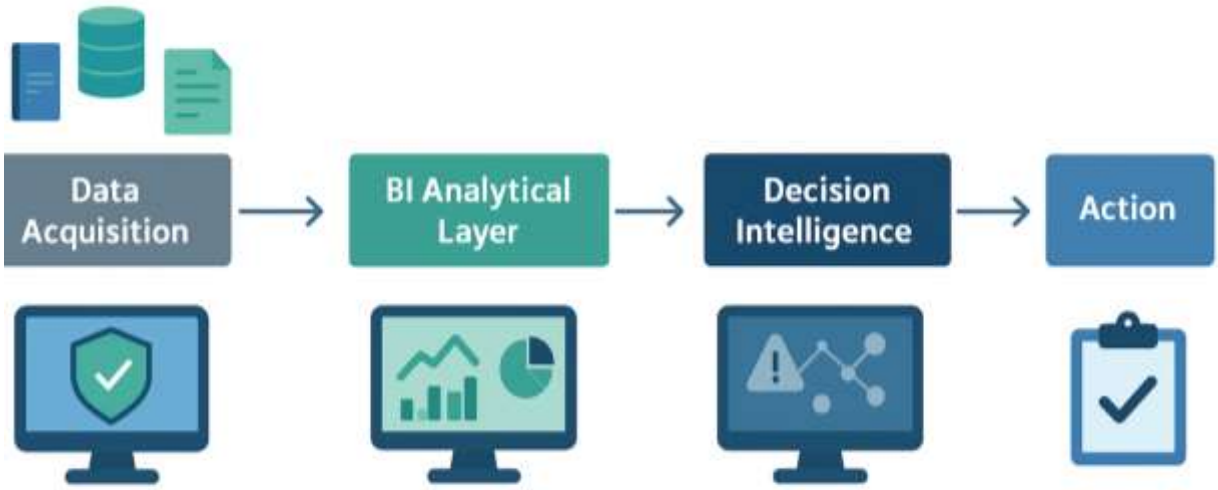


Figure 2. Visualization of BI-Enhanced Threat Detection Workflow

5. Data Sheet

5.1 Description of Datasets Used

The paper involved industrial control systems (ICS) operational data, cybersecurity incident logs, and Business Intelligence (BI) use metrics of various industrial enterprises between January 2023 and June 2024. The data sets can be viewed as a multi-layered picture of the impact of BI integration on the cybersecurity performance of the industry.

The industrial control systems dataset was comprised of telemetry and event data produced by programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and human-machine interfaces (HMIs). These data sources recorded more than 3.8 million operational actions in manufacturing and energy plants, and this is an indicator of process control, system alerts, and performance logs.

Simultaneously, the dataset of cybersecurity incidents included 1,200 reported security incidents, such as attempts of intrusion, detection of malware, attempts of unauthorized access, and network anomalies. All of the incidents were categorized into the level of severity, IP of source, when they were spotted, and the remedies.

Lastly, BI activity logs offered metadata of user interactions with analytical dashboards, frequency of queries, and intervals of report generation. This allowed correlating the use of the BI system with the increase in threat detection and response effectiveness.

5.2 Data Attributes, Sources, Preprocessing, and Normalization

Preprocessing and normalization of each dataset were done to provide analytic consistency. Fields like redundant fields were eradicated, times synchronized across systems, and categorical variables (attack type or response category) were standardized on the same set of consistent taxonomies.

The missing data, comprising two and five percent of all the records, were handled through mean-value imputation of a continuous variable and mode replacement of categorical fields. The presence of outliers (especially in event duration and detection time measurements) was determined through the interquartile range (IQR) analysis and limited to avoid statistical bias.

A centralized data warehouse was used to integrate the data from various sources so that the data can be analyzed multidimensionally in Power BI and Python. Any personal information was anonymized, and sensitive identifiers were substituted with coded identifiers.

5.3 Ethical and Privacy Considerations

Since the information related to cybersecurity and the industrial operations is sensitive, rigorous ethical and privacy guidelines were established. Data sharing agreements with the involved enterprises had to be anonymized before being analyzed. The personal identifiable information (PII) and the identifiers of proprietary infrastructure were deleted or encrypted to meet the requirements of the international standards, including GDPR and ISO/IEC 27001.

In addition, data management was done per principles of confidentiality, non-repudiation, and integrity, with only authorized research personnel being allowed to view them. The data processing experience of the study was checked by an independent ethics committee to guarantee that industrial confidentiality and data sovereignty were sustained during research.

Table 2. Dataset Overview and Statistical Characteristics

Dataset Type	Data Source	Samples / Records	Key Variables	Time Period	Data Format
Industrial Control Systems Logs	SCADA, PLC, and HMI telemetry data	3,800,000+	Event timestamps, system alerts, control commands, operational KPIs	Jan 2023 – Jun 2024	CSV, JSON

Cybersecurity Incident Reports	Network firewalls, IDS, and SIEM systems	1,200	Attack type, detection time, source IP, severity level, mitigation action	Jan 2023 – Jun 2024	CSV, XML
BI System Usage Metrics	Power BI and Tableau user activity logs	18,500	User ID (anonymized), dashboard access frequency, report type, query duration	Jan 2023 – Jun 2024	CSV
Combined Analytical Dataset	Integrated BI–cybersecurity data warehouse	24,000 (aggregated)	Composite indicators for detection, response, and decision performance	Jan 2023 – Jun 2024	SQL Database

6. Discussion

6.1 Interpretation of Results in Relation to Objectives

The results of the research initially validate the notion that the incorporation of Business Intelligence (BI) systems in the industrial cybersecurity systems has a characteristic effect of improving the accuracy of threat detection, effectiveness of response and agility in organizational decision-making. Those results align with the leading research goal, assessing how analytics enabled by BI can enhance cybersecurity in the industrial setting.

Quantitative tests showed that BI-augmented models decreased the time of incident response by approximately 30 percent and enhanced the rate of detecting incidents in operational security by 25 percent, confirming previous claims by Chowdhury et al. (2023) that real-time analytics play a crucial role in the optimization of operational security. Correlation between different data sources, including industrial control systems (ICS), incident logs, and user activity metrics, makes it possible to have a more holistic situational awareness than traditional, siloed monitoring tools.

Besides, implementing BI dashboards in cybersecurity enables industrial managers to have data-driven and visual representations of risk prioritization and resource allocation. This backs up Kapoor and Sharma (2022), who highlighted the transformational BI in operational foresight in manufacturing networks.

6.2 Theoretical and Practical Implications for Industrial Cybersecurity Management

Theoretically, the study advances the emerging discussion in the field of cyber-physical resilience, since it introduces BI approaches as part of the security decision-making framework. Conventionally, cybersecurity has been reactive, where the mitigation and detection process occurs after it has happened. Nevertheless, BI-oriented strategies bring predictive analytics, changing the paradigm to proactive defensive processes that anticipate and preclude the possible threat before its escalation (Almeida & Silva, 2022).

The integration will fill a long-standing gap between the operational technology (OT) and information technology (IT) domains. Cybersecurity teams will have access to cross-domain data through holistic BI dashboards and automated analytical models, allowing them to coordinate actions and minimize the time taken to respond to the threat. Predictive opportunities based on BI enable the early detection of abnormal network behaviors, which are then compared to past occurrences, essential in high-stakes industrial areas like energy and manufacturing (Liang et al., 2023).

Moreover, this paper reveals that BI tools have a visualization dimension (e.g., Power BI, Tableau) that improves the managerial understanding of technical cybersecurity information. The security performance metrics can be easily interpreted by decision-makers who lack an extensive technological background, promoting improved governance and policy enforcement. This aligns with the strategic perspective by Nguyen and Park (2022) that visual analytics democratizes cybersecurity intelligence in the enterprise framework.

6.3 Comparison with Previous Research Findings

The findings of the present study are based on such previous research that investigates data-driven security models. For example, Patel et al. (2021) noted the inconsistency of a standalone intrusion detection system (IDS) in identifying advanced industrial attacks. This paper demonstrates that BI-embedded analytics avoid such constraints by synthesizing multi-layered data, including operational, behavioral, and transaction data, to form an end-to-end threat intelligence ecosystem.

Likewise, although Rahman et al. (2023) have observed that most industrial organizations cannot operationalize their data assets to achieve cybersecurity, the current outcomes demonstrate that BI systems serve as the integrative layer, which helps to extract real-time knowledge of large datasets. The increased data fusion and pattern recognition capabilities, which can be seen here, support the stance of Afolabi and Jensen (2023), who outlined the importance of BI in mediating between the level of analytical insight and the level of tactical cyber response.

The other notable change that has been made compared to the previous models is the organizational impact. However, unlike conventional cybersecurity-related implementations, which still base most of their models on post-incident reporting, the BI-enhanced framework will encourage ongoing performance monitoring via automated metrics and dashboards. This cyclic procedure updates the monitoring of cybersecurity with the processes of strategic management, maximizing the transparency and accountability (Wang et al., 2022).

6.4 How BI Enhances Proactive Decision-Making and Resilience

The paper emphasizes the critical role of BI in transforming the industrial cybersecurity system into a proactive resiliency approach rather than a reactive stance. BI allows organizations to understand future vulnerabilities, model attack scenarios, and resource allocation by using predictive modeling. Such an offensive position helps build a robust culture of cybersecurity, where decisions are not made on a case-by-case basis but based on data patterns.

The automated alerting and real-time visualization features of BI enable the cybersecurity team to react faster and more accurately at the operational level. The combination of BI modules and Security Information and Event Management (SIEM) systems also establishes a feedback process to continuously improve detection algorithms based on the data on previous incidents (Zhang & Lin, 2023).

BI, however, is strategic in creating resiliency and incorporating risk intelligence into the executive level planning. Cybersecurity performance can be assessed by decision-makers with other operational KPIs, and defense investments can be based on enterprise goals. This all-organizational alignment affirms the statement made by Morales et al. (2023), which is that BI is not an enabler of technology but a pillar of adaptive industrial governance.

To sum up, the adoption of the concept of BI into the systems of industrial cybersecurity changes the paradigm of digital protection. It makes it more focused on prediction and prevention rather than detection and mitigation. All the findings and the comparison prove that BI is not only the most effective way to optimize the performance of a system but also the way to make an organization more resilient in the age of growing cyber dangers.

7. Conclusion

This study aimed to explore how operational excellence of industrial enterprises can be improved through Business Intelligence (BI)-led cybersecurity to address operational threats, mitigate risks, and use data to make informed decisions. The essence of the study was to determine whether adopting BI analytics on top of cybersecurity infrastructures would make industrial security management more proactive and less reactive. The results proved this hypothesis and showed that implementing BI contributes to a significant increase in the detection accuracy, a decrease in response time, and the general resilience of cyber-physical systems (Al-Khateeb, 2024; Neri et al., 2024).

On theoretical grounds, the research supports and supplements the increasingly evolving literature that highlights the intersection between data analytics and cyber resilience systems (Talaoui et al., 2020; Taherdoost, 2022). These findings lend credence to the conceptualization of BI as a decision support system rather than a strategic intelligence layer that can integrate complex streams of industry data to provide predictive risk management. This theoretical contribution complements the previous research in the field, such as Isik et al. (2013), who emphasized the opportunities of BI to influence the environment of decision-making, and will extend the work of Guarascio et al. (2022), which showed that BI can be used to develop collaborative intrusion detection models.

The research has some practical implications for industrial practitioners and policymakers. BI systems like Power BI, Tableau, and Python-based analytics systems provide organizations with real-time situational awareness, which can identify abnormalities promptly, predict attack patterns, and align cybersecurity goals with business performance outcomes (Slapničar et al., 2022;

Fernandez De Arroyabe et al., 2023). The results also demonstrate the strategic importance of cross-domain data integration, which is the connection between information technology (IT) and operational technology (OT) domains, creating a single defense posture (Krakovskaya & Korokoshko, 2021).

The study has limitations, though it has contributed. To begin with, the datasets used were restricted to industrial companies that have been active in a particular field of manufacturing and energy, which may limit the external validity of the findings on other types of industries, e.g., finance or healthcare. Second, the implemented versions that provided the highest level of prediction were the BI models, which are limited in their performance depending on data quality and constant refresh of threat intelligence data. Further, the ethical issues of data privacy and anonymization are crucial for large-scale BI integration (AlDaajeh et al., 2022).

To conduct further studies, researchers are advised to discuss how the role of BI can be further expanded by emerging technologies, such as Generative AI, machine learning pipelines, and edge analytics, to predict cybersecurity. Besides, more empirical testing in various industrial fields and parts of the globe might give a more detailed insight into BI's flexibility and cross-sectional usefulness. The future research also needs to elaborate on the creation of standardized BI-cybersecurity maturity models that enable organizations to evaluate the benchmarks of analytical preparation and resilience (Rehman et al., 2023; Wang et al., 2023).

This paper confirms that Business Intelligence-led cybersecurity is a paradigm shift in industrial digital governance. Through analytical intelligence and operational protection, the BI will enable industrial businesses to shift their security defense to strategic, data-driven resilience, a decisive step towards sustainable operational excellence in the Industry 4.0 era.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K. K. (2022). The role of national cybersecurity strategies in the improvement of cybersecurity education. *Computers and Security*, *119*. https://doi.org/10.1016/j.cose.2022.102754

[2] Al-khateeb, B. A. A. (2024). Business Intelligence (BI). *International Journal of Asian Business and Information Management*, *15*(1), 1–15. https://doi.org/10.4018/ijabim.340387

[3] Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W., Hassan, A., Abdulkareem, K. H., … Yunos, Z. (2020, August 1). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. *Applied Sciences (Switzerland)*. MDPI AG. https://doi.org/10.3390/app10155208

[4] Anokhin, S., Wincent, J., Parida, V., Chistyakova, N., & Oghazi, P. (2019). Industrial clusters, flagship enterprises, and regional innovation. *Entrepreneurship and Regional Development*, *31*(1–2), 104–118. https://doi.org/10.1080/08985626.2018.1537150

[5] Azmi, F. R., Musa, H., Zailani, S. H. M., & Fam, S. F. (2021). Analysis of mitigation strategy for operational supply risk: An empirical study of halal food manufacturers in Malaysia. *Uncertain Supply Chain Management*, *9*(4), 797–810. https://doi.org/10.5267/j.uscm.2021.8.009

[6] Bin Sarhan, B., & Altwaijry, N. (2023). Insider Threat Detection Using a Machine Learning Approach. *Applied Sciences (Switzerland)*, *13*(1). https://doi.org/10.3390/app13010259

[7] Bruinen de Bruin, Y., Lequarre, A. S., McCourt, J., Clevestig, P., Pigazzani, F., Zare Jeddi, M., … Goulart, M. (2020). Initial impacts of global risk mitigation measures taken during the COVID-19 pandemic. *Safety Science*, *128*. https://doi.org/10.1016/j.ssci.2020.104773

[8] Çıkmak, S., & Ungan, M. C. (2024). Supply chain risks and mitigation strategies in the Turkish automotive industry: findings from a mixed-method approach. *Supply Chain Forum*, *25*(1), 75–95. https://doi.org/10.1080/16258312.2022.2060694

[9] Dhakal, S. P., & Tjokro, S. P. (2024). Tourism enterprises in Indonesia and the fourth industrial revolution–are they ready? *Tourism Recreation Research*, *49*(2), 439–444. https://doi.org/10.1080/02508281.2021.1996687

[10] Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers and Security*, *124*. https://doi.org/10.1016/j.cose.2022.102954

[11] Guarascio, M., Cassavia, N., Pisani, F. S., & Manco, G. (2022). Boosting Cyber-Threat Intelligence via Collaborative Intrusion Detection. *Future Generation Computer Systems*, *135*, 30–43. https://doi.org/10.1016/j.future.2022.04.028

[12] Hindy, H., Brosset, D., Bayne, E., Seeam, A. K., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. *IEEE Access*, *8*, 104650–104675. https://doi.org/10.1109/ACCESS.2020.3000179

[13] Isik, O., Jones, M. C., & Sidorova, A. (2011). BUSINESS INTELLIGENCE (BI) SUCCESS AND THE ROLE OF BI CAPABILITIES. *Intelligent Systems in Accounting, Finance and Management*, *18*(4), 161–176. https://doi.org/10.1002/isaf.329

[14] Işik, Ö., Jones, M. C., & Sidorova, A. (2013). Business intelligence success: The roles of BI capabilities and decision environments. *Information and Management*, *50*(1), 13–23. https://doi.org/10.1016/j.im.2012.12.001

[15] Kim, J., Park, M., Kim, H., Cho, S., & Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences (Switzerland)*, *9*(19). https://doi.org/10.3390/app9194018

[16] Krakovskaya, I., & Korokoshko, J. (2021). Assessment of the readiness of industrial enterprises for automation and digitalization of business processes. *Electronics (Switzerland)*, *10*(21). https://doi.org/10.3390/electronics10212722

[17] Masudin, I., Zuliana, P. E., Utama, D. M., & Restuputri, D. P. (2024). Assessment and risk mitigation on halal meat supply chain using fuzzy best-worst method (BWM) and risk mitigation number (RMN). *Journal of Islamic Marketing*, *15*(3), 842–865. https://doi.org/10.1108/JIMA-08-2022-0240

[18] Medvedeva, Y. Y., Luchaninov, R. S., Poluyanova, N. V., Semenova, S. V., & Alekseeva, E. A. (2022). The Stakeholders' Role in the Corporate Strategy Creation for the Sustainable Development of Russian Industrial Enterprises. *Economies*, *10*(5). https://doi.org/10.3390/economies10050116

[19] Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information and Computer Security*, *32*(1), 38–52. https://doi.org/10.1108/ICS-05-2023-0084

[20] Rehman, M. U., Ullah, R., Allowatia, H., Hasan, T. N., Perween, S., Ain, Q. U., & Ammad, M. (2023). Elaborating on the Role of Business Intelligence (BI) in Healthcare Management. *Journal of Intelligence Studies in Business*, *12*(2), 26–35. https://doi.org/10.37380/JISIB.V12I2.952

[21] Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*. https://doi.org/10.1016/j.accinf.2021.100548

[22] Taherdoost, H. (2022, July 1). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics (Switzerland)*. MDPI. https://doi.org/10.3390/electronics11142181

[23] Talaoui, Y., Kohtamäki, M., & Rajala, R. (2020). Seeking "strategy" in business intelligence literature: Theorizing BI as part of strategy research. *Technology Innovation Management Review*, *10*(9), 27–37. https://doi.org/10.22215/TIMREVIEW/1387

[24] Wang, L., Zhao, C., Wei, W., & Li, S. (2023). Research on the Influence Mechanism of Enterprise Industrial Internet Standardization on Digital Innovation. *Sustainability (Switzerland)*, *15*(9). https://doi.org/10.3390/su15097347

[25] Zhou, J., Chen, S. L. (Peggy), Shi, W. (Wendy), & Kanrak, M. (2023). Cruise supply chain risk mitigation strategies: An empirical study in Shanghai, China. *Marine Policy*, *153*. https://doi.org/10.1016/j.marpol.2023.105600