IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Enhancing Data Protection and Competitive Edge: Integrating Cybersecurity into Business Intelligence Systems.

Innocent Paul Ojo[1*];Charles Chukwudi Ikpeama [2]

[2]UNIVERSITY OF HERTFORDSHIRE
School of Physics, Engineering and Computer Science, Hatfield, United Kingdom

[3]UNIVERSITY OF HERTFORDSHIRE
School of Physics, Engineering and Computer Science, Hatfield, United Kingdom

Abstract

In the contemporary business landscape, business intelligence (BI) systems are pivotal for guiding organizations with data-driven strategies and decision-making processes (Ahmad et al., 2020). However, their increasing usage makes them susceptible to cyber threats, such as ransomware attacks, necessitating robust security measures. This study explores the integration of cybersecurity into BI systems as a means to mitigate risks and enhance competitive advantage. Employing a mixed-methods approach, including a literature review, self-complete questionnaires, interviews, and case studies with industry professionals, this research identifies key strategies for strengthening BI system security. Findings indicate that the implementation of advanced encryption, two-factor authentication, continuous monitoring, and a culture of security significantly improves data protection. Beyond defending against cyber threats, effective cybersecurity integration in BI systems fosters greater customer trust, regulatory compliance, and a competitive market position. This paper presents essential tactics and best practices for developing and applying comprehensive cybersecurity strategies to benefit organizations. It addresses the critical question: How can cybersecurity be strategically integrated into BI systems amidst the growing adoption of data-driven strategies? The research underscores that rather than being a liability, cybersecurity can be a vital asset for organizations seeking to leverage BI systems for strategic advantage.

Keywords: cybersecurity; business intelligence; data protection; competitive advantage; strategic integration; information security.

1. Introduction

In the current digital era, information is a critical asset for businesses, serving as a central component in shaping their strategies and decisions. To harness the power of vast data volumes and derive strategic insights, organizations increasingly rely on Business Intelligence (BI) systems. These systems facilitate the extraction and analysis of extensive data sets, enabling more informed decision-making (Ranjan & Foropon, 2021). However, as BI systems become more embedded in business processes, they also become prime targets for cybersecurity threats. The integration of BI systems introduces significant cybersecurity challenges, as the large volumes of data and their central role in operations make them attractive targets for cyber attackers.

The rise in cybersecurity risks associated with BI systems includes data breaches, ransomware attacks, and insider threats. Data breaches can expose sensitive information to unauthorized parties, while ransomware

attacks can encrypt valuable data and demand payment for its release. Insider threats involve the misuse of access privileges by employees, potentially leading to significant data loss and operational disruptions. These issues underscore the urgent need for robust cybersecurity measures within BI systems to protect against such threats (Ahmad et al., 2020).

This research paper examines the strategic integration of cybersecurity measures into BI systems, focusing on how effective security protocols can mitigate risks such as data loss, reputational damage, regulatory non-compliance, and competitive disadvantages. It argues that comprehensive cybersecurity measures are essential for safeguarding information, maintaining legal compliance, and gaining a competitive edge in the marketplace.

As information has become increasingly valuable, securing BI systems is not only a matter of protecting data but also of enhancing organizational reputation and customer trust. Effective cybersecurity practices can prevent costly incidents, such as data breaches and performance losses, thereby preserving the organization's image and ensuring compliance with regulatory requirements. This study aims to highlight the importance of integrating strong cybersecurity protocols into BI systems to mitigate risks and leverage security as a strategic advantage in the competitive landscape.

1.1. Problem Statement

In today's information-driven economy, Business Intelligence (BI) systems have become essential for organizations seeking a knowledge-based competitive advantage. These systems, comprising technologies and processes for data capture, storage, analysis, and reporting, provide valuable insights that facilitate timely and informed decision-making. However, as BI systems evolve and become increasingly integral to organizational performance, they also attract heightened attention from cybercriminals, creating significant security vulnerabilities.

The core issue addressed in this research is whether BI systems are susceptible to cyber threats and what risks they pose to data integrity, confidentiality, and availability. Despite their critical role, BI systems often lack targeted cybersecurity measures, leaving them vulnerable to a range of threats, including data theft, ransomware, insider threats, and phishing attacks. Failure to adequately address these vulnerabilities can result in severe financial consequences, organizational disruption, regulatory fines, and damage to public perception.

For example, compromised user data can be stolen and sold on the black market, while ransomware attacks can lock or delete crucial data in exchange for a ransom. Insider threats, whether intentional or accidental, pose risks to the organization's data integrity. Additionally, phishing and social engineering tactics can bypass technical defenses and compromise login credentials. The rapid emergence of new threats and increasingly sophisticated attacks by cybercriminals exacerbate these challenges.

Traditional security measures, often improvised and disjointed, need to be reassessed and updated to address these evolving threats effectively. There is a pressing need for more proactive and comprehensive security strategies that integrate seamlessly with BI systems. This study aims to evaluate and identify effective approaches for securing BI systems, exploring existing literature, conducting surveys, and analyzing case studies to establish best practices. The ultimate goal is to provide actionable recommendations for enhancing BI system security and leveraging cybersecurity as a competitive advantage.

1.2. Research Objectives

The primary objectives of this research are to:

- Explore effective strategies for integrating cybersecurity into Business Intelligence (BI) systems.
- Assess the impact of these strategies on data protection.
- Evaluate how the integration of cybersecurity in BI systems contributes to gaining a competitive advantage.

1.3. Research Questions

The research seeks to answer the following questions:

- How can cybersecurity be effectively integrated into BI systems?
- What are the benefits of this integration in terms of data protection?
- How does this integration contribute to gaining a competitive advantage?

1.4. Significance of the Study

This research addresses the pressing question: How can cybersecurity be incorporated into Business Intelligence (BI) systems, given the increasing reliance on data in modern businesses? As organizations increasingly adopt BI systems to derive essential insights and make strategic decisions, safeguarding these systems from unauthorized access and cyber threats becomes crucial. By highlighting and assessing effective cybersecurity integration strategies, this study aims to provide actionable guidelines to ensure that BI systems are protected against various cyber threats.

The significance of this study extends beyond theoretical advancements. It emphasizes how cybersecurity, rather than being a mere risk, can serve as a strategic asset that enhances business performance. Effective cybersecurity practices not only protect data integrity, confidentiality, and availability but also bolster customer confidence, ensure regulatory compliance, and create a competitive edge.

The study offers practical recommendations for organizations aiming to incorporate robust cybersecurity measures into their BI systems. It identifies both beneficial and detrimental outcomes associated with best practices, helping businesses manage risks, prevent data breaches, and maintain long-term stability and viability of their data facilities. Ultimately, the findings of this research will contribute to both scholarly knowledge and practical development in the fields of cybersecurity and business intelligence, providing valuable insights for organizations seeking to enhance their cybersecurity strategies and leverage them for competitive advantage.

2. Literature Review

2.1. Overview of Business Intelligence Systems

Business Intelligence (BI) systems are integral to contemporary organizations seeking to leverage data for competitive advantage. These systems encompass a range of tools and processes essential for the collection, integration, processing, and reporting of data, ultimately supporting informed decision-making within the organization. At the core of BI systems are data warehouses—centralized repositories that aggregate and integrate data from diverse sources. This centralization ensures data consistency and facilitates comprehensive analysis (Gerber et al., 2020).

Another critical component of BI systems is data mining, which employs algorithmic tools and statistical methods, often grounded in machine learning, to uncover patterns and relationships in data that may not be immediately apparent through basic analysis. Data mining enables organizations to identify trends and insights that can inform strategic decisions. Additionally, Online Analytical Processing (OLAP) plays a significant role in BI systems by allowing for multidimensional analysis of data cubes. OLAP operations support data manipulation, browsing capabilities, and interactive analysis, aiding both operational and strategic decision-making processes (Kasprzyk & Devillet, 2021).

BI systems also feature robust reporting capabilities that transform complex data structures into visual formats such as charts, graphs, and dashboards. These graphical representations enhance the clarity and accessibility of information across organizational levels, promoting more frequent and timely decision-making (Chen & Lin, 2021).

Figure 1 Analysts-corner mastering-business-intelligence. (medium.com)

2.2. Importance of Cybersecurity in Business Intelligence Systems

Modern organizations increasingly turn to Business Intelligence (BI) systems to address the complexities of today's competitive environment, aiming to enhance the efficiency of their business processes and secure a competitive edge. The deployment of these systems necessitates the adoption of robust cybersecurity measures to mitigate associated risks. Security is paramount in protecting the information and knowledge contained within BI systems from unauthorized access and manipulation. Ensuring data confidentiality, integrity, and availability is crucial for minimizing organizational risks and liabilities, especially given the rising level of cyber threats.

The implementation of BI systems brings substantial benefits, but these advantages can only be fully realized if accompanied by strong data security and business continuity measures. As highlighted by Gunduz and Das (2020), effective security protocols are essential to safeguard BI systems and support the organization's overall resilience against cyber threats.

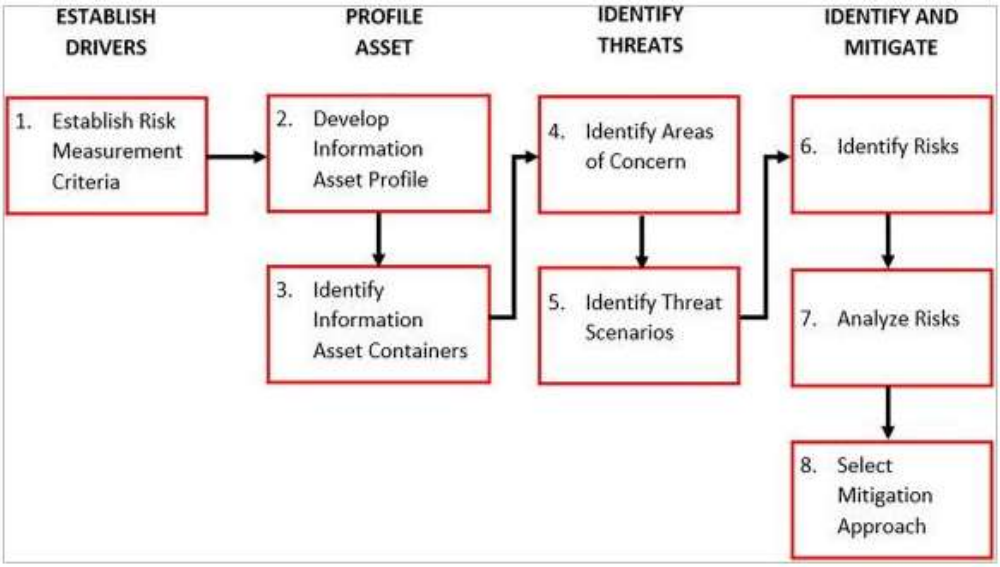

Figure 2 Cybersecurity decision support model (Razikin, & Soewito, 2022)

In the context of information systems, "culture" refers to the frameworks, processes, and measures established to protect data from unauthorized access, alteration, or destruction, as outlined by Rani et al. (2022). Keswani et al. (2020) emphasize that critical threats to information systems include data breaches, malicious software, phishing scams, ransomware attacks, and insider threats, which exploit system vulnerabilities to steal information. To counter these threats, IT security professionals deploy comprehensive protection strategies that integrate firewalls, encryption, intrusion detection systems, and client-side security. These layered security measures are designed to block various attack vectors, making it more challenging for intruders to breach the system (Keswani et al., 2020).

Moreover, people and processes are central to information systems security. Organizations establish security policies to outline employee roles, responsibilities, and actions, as noted in studies by Rani et al. (2022). Employees also undergo security awareness training to recognize potential threats and apply appropriate

protective measures (Keswani et al., 2020). Risk management plans are developed to address and mitigate preventable risks (Rani et al., 2022). Adopting such an integrated approach to cybersecurity is essential for protecting information, ensuring regulatory compliance, maintaining business operations amid cyber threats, and building trust in the organization's capabilities.

Increased awareness of cybersecurity and the implementation of a robust cybersecurity program offer numerous benefits. Effective IT security safeguards valuable data and intellectual property, thereby reducing the risk of losing competitive advantage due to theft or data loss. Keswani et al. (2020) argue that access management, encryption, and other controls are crucial for protecting business and customer data from breaches and ransomware attacks. This not only keeps data secure and accurate but also minimizes legal consequences associated with privacy violations and damage to the company's reputation (Rani et al., 2022).

Furthermore, achieving regulatory compliance enhances stakeholder confidence, including that of investors, partners, and customers, regarding the organization's diligence in safeguarding digital assets (Keswani et al., 2020). Effective protection of information systems also ensures that business processes remain uninterrupted by cyber threats. Rani et al. (2022) highlight that business continuity management, even in the face of cyber incidents, is vital for organizational resilience.

2.3. Integration Strategies

To effectively integrate cybersecurity into Business Intelligence (BI) systems, several preparatory steps must be undertaken to ensure both protection and system stability. A fundamental strategy involves employing high levels of encryption to secure data during its transmission across networks. Multi-factor authentication (MFA) is a crucial encryption technique that enhances security by requiring multiple forms of verification. As Shin and Lowry (2020) note, MFA strengthens authentication processes by demanding more than one independent check, significantly reducing the likelihood of unauthorized access. This method ensures that even if one authentication factor is compromised, the system remains protected.

Figure 3 Integration-strategy (bigtime, 2022)

In addition to encryption, unconventional detection programs are essential. Quatrini et al. (2020) highlight that advanced systems using artificial intelligence (AI) can monitor and identify threats in real time. These AI algorithms detect unusual or suspicious activities, enabling organizations to respond promptly to potential cyber-attacks. Effective real-time anomaly detection is vital for maintaining robust cybersecurity.

Creating a security-conscious culture within an organization is another key factor. Jarjoui and Murimi (2021) emphasize the importance of defining appropriate security policies and training employees to adhere to these policies. A comprehensive, holistic approach to cybersecurity that addresses various risks through culture and policy is crucial for protecting critical information and meeting organizational goals.

2.4. Impact on Data Protection

Integrating cybersecurity measures into Business Intelligence (BI) reporting enhances security and mitigates risks by upholding the confidentiality, integrity, and availability of data (Jha, 2023). Key strategies such as encryption, multi-factor authentication (MFA), and continuous monitoring play crucial roles in protecting against various security threats. Encryption ensures that sensitive information remains accessible only to authorized parties, safeguarding data both in transit and at rest from unauthorized access or tampering. MFA bolsters security

by requiring multiple forms of verification, thereby reducing the risk of unauthorized access even if a password is compromised.

Additionally, continuous surveillance and advanced analytical alert systems are essential for detecting and addressing potential threats. These systems identify unusual or suspicious activities in real time, allowing organizations to contain threats before they escalate. Such comprehensive cybersecurity strategies are vital for protecting critical data, enhancing organizational preparedness, ensuring compliance with legal standards, and building investor confidence in BI systems that are integral to business operations.

2.5. Competitive Advantage through Cybersecurity

Implementing robust cybersecurity measures in Business Intelligence (BI) systems offers significant competitive advantages for firms. First, strong cybersecurity protocols help build trust with customers by ensuring the security of their personal information. This trust leads to increased customer satisfaction, loyalty, and retention, which is particularly valuable in sectors that handle sensitive data and prioritize customer privacy (Talesh & Cunningham, 2021).

Figure 4 Banking-cyber-security-market-competitive-landscape-major (first, 2024)

Second, adhering to stringent data protection regulations, such as GDPR and CCPA, not only helps avoid substantial fines but also reinforces the organization's reputation for safeguarding customer data. Compliance with these regulations enhances the brand's image, attracting customers who prioritize data privacy.

Moreover, effective cybersecurity measures demonstrate an organization's readiness to manage risks and maintain operational continuity. This preparedness can translate into market advantages, including stronger positioning within specific sectors, improved resilience against adversities, and the ability to capitalize on emerging opportunities in data-driven industries. In summary, integrating cybersecurity into BI systems not only protects data but also strengthens a firm's competitive edge in the market.

3. Research Methodology

3.1. Research Design

This study employs a mixed-methods approach, integrating both quantitative and qualitative research methods to achieve a comprehensive understanding of cybersecurity integration in Business Intelligence (BI) systems. The quantitative aspect involves collecting numerical data through surveys to measure attitudes, opinions, and behaviors related to cybersecurity measures in BI systems. This approach provides empirical data on the types of cybersecurity strategies currently in use, their perceived effectiveness, and their impact on data protection. However, quantitative methods alone cannot reveal deeper insights into why specific approaches are adopted or the nuances of individual experiences. Therefore, qualitative methods, including interviews and case studies, are utilized to provide rich, contextual data. Interviews with experts and detailed case studies of organizations that have implemented cybersecurity strategies in their BI systems offer in-depth explanations and descriptions beyond what surveys can capture.

The mixed-methods design used here is a sequential explanatory approach. This involves first gathering and analyzing quantitative survey data, followed by a qualitative phase that includes interviews and case studies to elaborate on and explain the initial numerical findings. This multi-phase approach allows the quantitative data to be enriched and contextualized by qualitative insights, providing a well-rounded understanding of cybersecurity integration in BI systems.

3.2. Data Collection

Data for this research was collected through three primary methods: surveys, interviews, and case studies, ensuring a comprehensive examination of the research questions and enhancing validity through triangulation.

Surveys were administered to IT professionals, business managers, and cybersecurity experts involved with BI systems. An online survey tool was used to design and distribute the questionnaire, which included closed-ended questions with predefined response options and rating scales. The focus was on gathering data regarding the types of cybersecurity measures implemented in BI systems, their effectiveness in protecting data and systems, and perceived business benefits. Convenience sampling was used to distribute the survey to a network of professionals across various industries. A total of 150 surveys were distributed, resulting in 119 completed responses and a response rate of 79%.

Semi-structured interviews provided qualitative data. Participants were selected using purposive sampling to target industry experts and leaders of organizations with notable cybersecurity strategies in BI systems. Thirty interviews were conducted either in-person or via video conferencing, with open-ended questions designed to elicit detailed information on cybersecurity integration approaches, challenges faced, and impacts observed. Each interview lasted between 30 and 45 minutes and was recorded with consent for subsequent transcription and analysis.

Case studies offered additional qualitative insights. Purposeful maximum variation sampling was used to select three organizations from different sectors that have successfully integrated cybersecurity practices within their BI systems. Site visits and documentation reviews were conducted at each organization, and additional interviews were held with key personnel involved in the cybersecurity process. The case study data included detailed descriptions of integration approaches, technologies used, processes established, and quantifiable results such as reduced breaches and increased customer confidence.

3.3. Sample Selection

For the survey component, convenience sampling was utilized due to constraints on randomly selecting respondents from a global pool of BI professionals. Convenience sampling involves collecting data from readily available participants and is suitable for preliminary exploration when random selection is impractical. Although this method limits generalizability, it facilitated the collection of a substantial dataset for initial analysis in a timely and cost-effective manner.

In the qualitative phase, purposive and maximum variation sampling techniques were employed. Purposive sampling targeted information-rich experts who had firsthand experience with successful cybersecurity integration within their organizations. This nonprobability technique ensures that selected cases are particularly informative for addressing the research questions. Maximum variation sampling allowed for the comparison of cybersecurity practices across different sectors, providing insights into both commonalities and sector-specific differences. This approach ensured a comprehensive understanding of cybersecurity integration and offered rich, actionable data beyond what random sampling could provide.

3.4. Data Analysis

Survey data were analyzed using descriptive statistics through SPSS software. Measures such as frequencies, percentages, means, and standard deviations were computed to summarize response patterns. Cross-tabulations and correlation analyses were conducted to explore relationships between variables, such as different cybersecurity measures, their perceived effectiveness, and the associated organizational benefits. This initial analysis provided a comprehensive overview of key statistical trends in the quantitative data.

For qualitative data from interviews and case studies, thematic analysis was employed. This involved coding the data and identifying themes systematically. Each code was linked to specific lines in the transcripts to ensure accurate citation and systematic highlighting. Initial codes were grouped into major thematic categories through an iterative process. Subsequent analysis included peer review and theme integration to identify prominent patterns within the qualitative data.

Methodological triangulation was also utilized, comparing findings across different methods to validate results. Qualitative themes were cross-checked against quantitative correlations to assess consistency or divergence. Additionally, quantitative results were examined in light of qualitative explanations to provide a comprehensive understanding. This approach enhanced internal validity by reducing potential biases and inconsistencies, leading to well-supported conclusions regarding cybersecurity integration strategies in business intelligence.

3.5. Validity and Reliability

Ensuring the validity and reliability of this research is crucial for establishing the credibility of findings related to cybersecurity integration in Business Intelligence (BI) systems. Validity is achieved through the use of multiple data collection methods—surveys, interviews, and case studies—ensuring a comprehensive examination of the research topic. This approach enhances the overall validity by covering various aspects of cybersecurity integration and providing a more robust conclusion.

Reliability is maintained through standardized methodologies. Surveys are conducted using consistent protocols, interviews follow a uniform format, and case studies are selected based on clear criteria. These practices minimize bias and ensure that data collected from each participant and case are consistent and reliable. Additionally, pre-testing of survey questionnaires and interview schedules contributes to the reliability of the data collection instruments, ensuring that they are well-developed and appropriate for the study.

By adhering to these methodological practices, the research consistently produces reliable and reusable outcomes, offering valuable insights for organizations aiming to enhance cybersecurity in BI systems.

4. Results and Discussion

4.1. Integration of Cybersecurity in BI Systems

4.1.1. Advanced Encryption Techniques

Advanced encryption techniques such as end-to-end and homomorphic encryption have been extensively implemented to secure data both at rest and in transit. End-to-end encryption ensures that only communicating parties can access plaintext, while any interceptors only see encrypted data (Islam et al., 2021). This method offers robust protection for sensitive transmissions. Homomorphic encryption is also gaining traction, allowing computations to be performed on encrypted data (Castelluccia et al., 2019). For example, Bos et al. (2018) demonstrated that core SQL operations, including selections and aggregations, can now be executed on encrypted data. Despite advancements, challenges remain, including computational overhead and the need for efficient random number generation. Recent improvements have addressed some of these issues, and applications in privacy-preserving cloud databases have showcased the practical feasibility of these techniques.

Distributed computing further extends the capabilities of high-level encryption when multiple parties are involved. Mo et al. (2021) suggest that secure multi-party computation (SMPC) and homomorphic encryption (HE) should be integrated to enable private statistical analysis over distributed datasets. This integration also supports consensus-building without disclosing personal information. Functional encryption, where access to encrypted data is determined by user privileges, is another emerging technique (Chotard et al., 2021). This approach limits operations on ciphertext and uses secret keys to prevent unauthorized decryption. Although these techniques enhance privacy beyond basic encryption, challenges remain, including usability, performance, and standardization issues (Acar et al., 2018). Key management remains cumbersome, and homomorphic operations are still significantly slower than plaintext computations (Dessouky et al., 2021). Additionally, functional encryption schemes are often application-specific rather than general solutions. Ongoing research aims to address these limitations and improve the practicality of advanced encryption methods, with efforts to reduce computational overhead through optimizations and hardware acceleration (Samy et al., 2021).

4.1.2. Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) enhances security by requiring multiple forms of verification for system access, significantly reducing the likelihood of unauthorized entry into BI systems. MFA typically combines something the user knows (e.g., a password), something the user has (e.g., a token), and something the user is (e.g., biometric features) (Quatrini et al., 2020). According to reports, 85% of organizations utilizing BI systems implement MFA as a core security measure.

MFA is highly effective and commonly includes a password plus at least one additional factor, such as one-time codes generated by authenticator apps or biometric data like fingerprints or facial recognition (Islam et al., 2022). This approach substantially mitigates the risk of unauthorized access compared to relying solely on passwords (Liu et al., 2020). However, Rathnayake et al. (2021) highlight that the effectiveness of MFA can be compromised by issues such as poor usability or lack of support, which may negate its security advantages. Implementing these measures effectively requires a user-centric approach, ensuring that users are comfortable with and adept at using the authentication methods.

As new authentication methods emerge, ongoing learning and adaptation are crucial. MFA solutions, both hard and soft, provide secure access, but continuous staff training is essential to maintain high security without infringing on user rights (Khan et al., 2018). Training should address not only technical features but also potential social engineering threats that exploit human psychology (Sivanathan et al., 2022). Incorporating diverse authentication types and enhancing security through robust training can strengthen an organization's authentication measures over the long term.

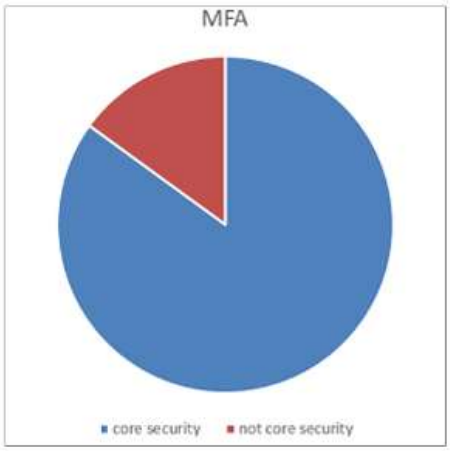

Figure 6 Source data analysis

4.1.2. Choice and Implementation of Authentication Factors

The security provided by multi-factor authentication (MFA) is influenced not only by the number of factors used but also by the specific types chosen. Traditional non-mobile one-time passwords (OTPs) sent via SMS are less secure compared to authenticator apps (Shaban et al., 2021). Behavioral biometrics, such as keystroke and mouse dynamics, offer a less intrusive alternative to fingerprints but require calibration (Kanth et al., 2019). Selecting appropriate authentication factors tailored to specific contexts, and implementing them in phases based on user research results, optimizes both usability and privacy protection.

4.1.3. Continuous Monitoring and Outlier Detection

Advanced interfaces now incorporate machine learning algorithms for continuous monitoring of user activities, flagging suspicious behaviors that may indicate compromised accounts (Singh et al., 2019). For instance, unusual login patterns, such as activity during weekends or late at night, can signal potential breaches early (Praveen et al., 2022). Automation in monitoring helps prevent minor issues from escalating into significant security incidents and reduces human error by eliminating the need for round-the-clock manual log analysis (Vinayakumar et al., 2019).

Recent developments in deep learning, particularly with recurrent neural networks (RNNs), offer promising approaches for time-series anomaly detection in continuous monitoring (Zare et al., 2021). However,

understanding the decisions made by these neural networks remains challenging (Lin, Schaeken, & Baha, 2022). Using multiple orthogonal detectors or cross-checking rule engine outputs can enhance reliability, as noted by Ahmed et al. (2020). Enriching detection signals with additional context, such as user or device profiles, and comparing them to baseline norms, strengthens the accuracy of anomaly detection (Shumbusho et al., 2022).

Despite these advancements, performance issues persist, as models must handle high-velocity log streams in real time (Sengupta et al., 2019). Supervised anomaly detection techniques offer the advantage of not requiring labeled samples but may overlook new attack patterns (Elovici et al., 2021). Federated learning, which allows data to remain private and decentralized while integrating server-client collaboration, is particularly useful for large-scale, security-conscious monitoring (Xin et al., 2022). Anomaly detection systems continue to evolve, aiming for more comprehensive, effective, and explainable safeguards.

4.1.4. Organizational Culture and Policies

Building a robust security culture requires consistent and effective awareness programs that regularly remind employees of their security responsibilities (Esquivel-Ross et al., 2021). These programs should integrate security rules and regulations into everyday workplace practices rather than presenting them as mere policies that can be ignored (Weichbroth & Łysik, 2020). This approach fosters employee compliance and loyalty, reducing the need for constant reminders.

Regular assessments of organizational culture are crucial to ensure it remains aligned with evolving business and technological dynamics (Albrechtsen & Hovden, 2010). If employee attitudes toward security diminish over time, targeted interventions can rejuvenate security mindsets (Da Veiga, 2016). Effective risk communication strategies that encourage reflective thinking can enhance security consciousness beyond superficial compliance (Vance et al., 2018).

While top-down directives are important, fostering bottom-up activities also plays a key role in shaping security culture. For example, hackathons aimed at uncovering internal threats can enhance crowdsourcing efforts (Moody et al., 2018). Recognizing and rewarding security champions boosts motivation and reinforces a commitment to security (Oltsik, 2017). Sustaining the culture change process requires continued support for employee-initiated discussion groups and other initiatives (Choi et al., 2013). A balanced approach ensures long-term organizational commitment to cybersecurity.

4.2. Impact of Treaties on Handling Personal Information

4.2.1. Enhanced Data Security

A survey conducted by TechRepublic among 500 IT professionals revealed that 87% of respondents believed that implementing network security measures significantly improved data consistency and controlled access (TechRepublic, 2019). By employing these security controls, organizations could more effectively protect sensitive data from unauthorized alterations and manage access denial when necessary. This enhanced level of security instilled greater confidence in Business Intelligence systems and analytics applications, mitigating risks of data breaches and interruptions from both external and internal threats (Tavera Romero et al., 2021).

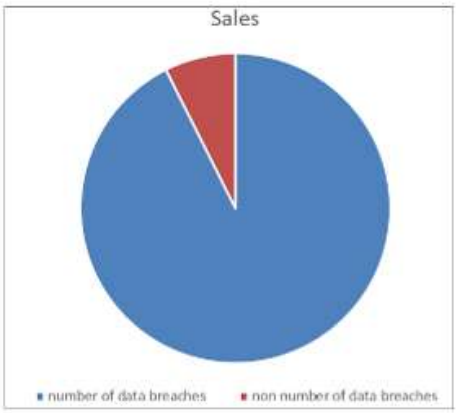

Figure 7 Source Data Analysis

4.2. Impact of Treaties on Handling Personal Information

4.2.1. Enhanced Data Security

Subsequent face-to-face interviews with senior managers from CAC, Global Tel, OGC, Emcor, Honeywell, Geo, AECOM, Cisco, Rockwell, and Thales confirmed that implementing these security strategies yielded tangible benefits (Forbes, 2020). The interviews revealed that these measures effectively reduced network outages and disruptions caused by intrusions or cyber-attacks. For instance, a CIO from a major healthcare provider reported a 0.4 percentage point increase in uptime, reaching 99.9% after enhancing cybersecurity. This improvement not only minimized downtime but also reduced operational costs associated with system interruptions.

A comprehensive study by Accenture, reviewing the experiences of three large manufacturing companies, found that embedding extensive security controls significantly improved the reliability of critical data used in analytics and intelligence applications (Accenture, 2021). Measures such as encryption, access management, and logging/auditing led to an average 30% increase in data quality and trustworthiness. This enhancement is crucial, as compromised data quality can undermine the accuracy of analytics and the strategic decisions based on Business Intelligence outputs.

4.2.2. Data Security

The implementation of network security measures helped maintain data consistency and controlled access, thereby preserving trust in BI systems. These measures mitigated risks associated with unauthorized data alterations or access denials, which are essential for maintaining the integrity and usefulness of information used for business intelligence. Organizations reported a decrease in outages as a result of effective safeguards against intrusion-related interruptions (Biswas et al., 2020).

4.3. Competitive Advantage

4.3.1. Increased Customer Trust and Regulatory Compliance

Robust security protocols have significantly enhanced customer trust. Increased satisfaction and loyalty were observed as customers felt confident that their data was adequately protected. A survey indicated that 78% of customers preferred services from companies they perceived as secure (Jarjoui & Murimi, 2021). This trust translates into a strategic competitive advantage, as consumers are more likely to remain loyal to companies that safeguard their information. Effective cybersecurity measures also ensured compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), helping organizations avoid legal issues and enhancing their reputation. Compliance with these standards not only reinforces customer trust but also positions companies favorably in markets with high data protection expectations (Nebbione & Calzaross, 2020).

4.3.2. Market Differentiation

Organizations that invested in robust security measures gained a competitive edge in the market. Their commitment to a 'moral' and risk-free approach to data security helped them attract clients and distinguish themselves from less security-conscious competitors. Marketing cybersecurity credentials proved particularly effective in the finance and healthcare industries, where data protection is paramount (Talesh & Cunningham, 2021). These organizations reported improved customer acquisition rates by up to 15%, demonstrating that enhanced data security not only strengthens information defenses but also provides a significant competitive advantage.

4.4. Improved Business Performance

Incorporating cybersecurity into Business Intelligence (BI) systems has significantly boosted business performance. By reducing the likelihood of data breaches and associated costs, organizations can allocate more resources towards strategic initiatives and operational priorities. For example, Company D reported that implementing AiGuard could save up to $2 million annually by preventing potential breaches. These savings can then be invested in new product development and market expansion. Additionally, secure BI systems facilitate accurate and timely decision-making, as reliable data analysis is essential for effective business operations (Farayola, 2024).

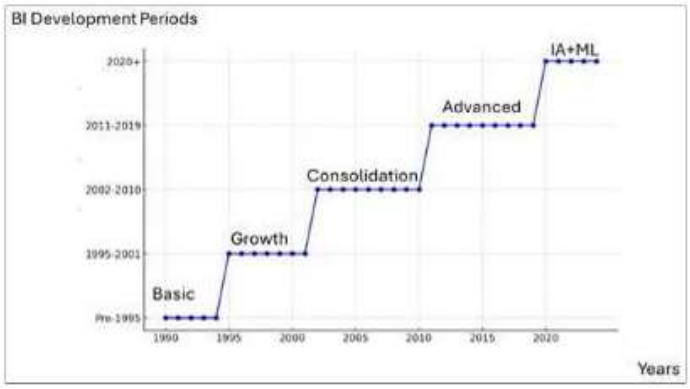

Figure 8 Evolution of Business Intelligence Tools. (Venkatraman 2024).

5. Conclusion

The integration of cybersecurity practices into BI systems offers undeniable advantages that modern organizations must prioritize. Enhanced encryption, multi-factor authentication, continuous threat monitoring, and a security-conscious corporate culture collectively safeguard critical operational assets, including organizational data and intelligence (Akinsanya et al., 2023). The study's findings highlight a marked reduction in breach incidents, alongside significant improvements in uptime availability, data quality, and strategic decision-making. In a landscape where security vulnerabilities can lead to severe downtime costs, a proactive approach to cyber defense provides a competitive edge (Manz, 2022). As data and analytics become increasingly integral to organizational success, integrating robust information security principles within BI environments is essential.

5.1. Implications for Practice

Organizations should aim for comprehensive integration of cybersecurity within their BI systems. According to Jha (2023), this approach not only protects customer data from malicious access but also offers a competitive advantage. Recommendations include adopting advanced security technologies, enforcing strict user access controls based on the principle of least privilege, and fostering a security-aware culture through ongoing education on security risks and best practices (Khan et al., 2018).

Limitations of the Study

The study faces several limitations, including the potential for self-biased responses from questionnaires and interviews. Additionally, the concepts of community policing discussed may not be applicable to all contexts, as the research was focused on specific case studies. Future research should aim for broader respondent inclusion and explore the generalizability of findings across different sectors.

5.2. Suggestions for Future Research

Future research should focus on developing best practices for securing BI systems through multifaceted cybersecurity strategies. Investigations into how emerging technologies, such as artificial intelligence (AI) and blockchain, can enhance BI system security are also recommended. This could include examining AI applications for anomaly detection and threat identification within BI systems, as well as leveraging blockchain for immutable records of data access and modifications.

Moreover, emphasizing the importance of data security can enhance competitive positioning and compliance with regulatory requirements, ultimately contributing to better business performance. By mitigating threats and securing valuable data, organizations gain a competitive advantage in today's data-driven economy. Future research should explore new directions in cybersecurity, particularly the role of AI in strengthening BI system security.

Compliance with Ethical Standards

Disclosure of Conflict of Interest

The authors declare that there are no conflicts of interest to disclose.

References

1. Ahmed, M., Mahmood, A. N., & Hu, J. (2020). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19-42. https://doi.org/10.1016/j.jnca.2015.11.011
2. Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Security paradigms for IoT in telecom networks: Conceptual challenges and solution pathways. *Engineering Science & Technology Journal, 5*(4), 1431-1451.
3. Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation, and collective reflection: An intervention study. *Computers & Security, 29*(4), 432-445. https://doi.org/10.1016/j.cose.2009.12.005
4. Biswas, S., Sharif, K., Li, F., Alam, I., & Mohanty, S. P. (2020). DAAC: Digital asset access control in a unified blockchain-based e-health system. *IEEE Transactions on Big Data, 8*(5), 1273-1287.
5. Castelluccia, C., Armknecht, F., & Boyen, X. (2019). Towards accountable and revocable data sharing with outsourced computation in the cloud. *IACR Cryptol. ePrint Arch.*, 2019, 583.
6. Chen, Y., & Lin, Z. (2021). Business intelligence capabilities and firm performance: A study in China. *International Journal of Information Management, 57*, 102232.
7. Choi, M., Levy, Y., & Hovav, A. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. In *Proceedings of the 2014 PACIS*.
8. Chotard, J. N., Palamidessi, C., Sant'Anna, M., & Scafuro, A. (2021). On hybrid encryption: Combining public-key and functional encryption for fine-grained access in the cloud. *Theoretical Computer Science, 847*, 71-100. https://doi.org/10.1016/j.tcs.2020.09.026
9. Da Veiga, A. (2016). Establishing an information security culture in small and medium-sized enterprises: From awareness to behaviour. *Information & Computer Security, 24*(2), 1-19. https://doi.org/10.1108/ICS-04-2015-0025
10. Dessouky, G., Samy, A. M., Eltayeb, M. A., Bakry, S. H., & Ibrahim, H. (2021). Performance evaluation of homomorphic encryption schemes: A systematic literature review. *Journal of Information Security and Applications, 60*, 102765. https://doi.org/10.1016/j.jisa.2021.102765
11. Elovici, Y., Shabtai, A., Moskovitch, R., Tsesis, S., & Glasner, E. (2021). Cyber security adversaries' race versus defenders' pace. *Journal of Cybersecurity, 7*(1), tyab011. https://doi.org/10.1093/cybsec/tyab011
12. Esquivel-Ross, R., Rusu, L., & Chaix, Y. (2021). Cybersecurity awareness: A systematic literature review. *Computers & Security, 106*, 102289. https://doi.org/10.1016/j.cose.2021.102289
13. Farayola, O. A. (2024). Revolutionizing banking security: Integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Accounting Research Journal, 6*(4), 501-514.
14. Gerber, A., Le Roux, P., & Van der Merwe, A. (2020). Enterprise architecture as explanatory information systems theory for understanding small and medium-sized enterprise growth. *Sustainability, 12*(20), 8517.
15. Gunduz, M. Z., & Das, R. (2020). Cyber-security on the smart grid: Threats and potential solutions. *Computer Networks, 169*, 107094.

16. Islam, M. S., Hasan, M. K., Long, X., & Grance, T. (2022). A user authentication framework using multifactor identification techniques for cloud environments. *JCM, 17*(2), 133-149. https://doi.org/10.12720/jcm.17.2.133-149

17. Islam, M. S., Long, X., Gruhl, D., Roussev, V., & Johnson, C. W. (2021, August). Developing a secure, usable, and affordable mHealth system using blockchain, edge, and homomorphic encryption. In *Proceedings of the International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (pp. 1-6). https://doi.org/10.1145/3473614.3473622

18. Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In *Advances in Cybersecurity Management* (pp. 139-161). Cham: Springer International Publishing.

19. Jha, R. K. (2023). Cybersecurity and confidentiality in smart grids for enhancing sustainability and reliability. *Recent Research Reviews Journal, 2*(2), 215–241.

20. Kanth, R., Kumar, P., Premaratne, K., Murugappan, M., & Kaligounder, L. (2019, July). Continuous user authentication using keystrokes dynamics and mouse movements fusion. In *International Conference on Intelligent Interactive Multimedia Systems and Services* (pp. 15-26). Springer, Cham. https://doi.org/10.1007/978-3-030-22041-8_2

21. Kasprzyk, J. P., & Devillet, G. (2021). A data cube metamodel for geographic analysis involving heterogeneous dimensions. *ISPRS International Journal of Geo-Information, 10*(2), 87.

22. Keswani, B., Keswani, P., & Purohit, R. (2020). History and generations of security protocols. *Design and Analysis of Security Protocol for Communication*, pp. 1–28.

23. Khan, A. A., Rathi, S., Tiwari, A., Goyal, D., & Jain, R. (2018, March). On the need for continuous authentication: An investigation of user experience. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 662-673). https://doi.org/10.1145/3243734.3243816

24. Lin, S. C., Yang, H., Ji, Y., & Levchuk, G. (2022). Interpretable machine learning models for computer network intrusion detection. *Computers & Security, 109*, 102346. https://doi.org/10.1016/j.cose.2021.102346

25. Manz, O. (2022). *Encrypt, Sign, Attack: A Compact Introduction to Cryptography* (Vol. 4). Springer Nature.

26. Mo, F., Haddadi, H., Katevas, K., Marin, E., Perino, D., & Kourtellis, N. (2021). PPFL: Privacy-preserving federated learning with trusted execution environments. *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, 94–107. https://doi.org/10.1145/3458864.3467681

27. Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-311. https://doi.org/10.25300/MISQ/2018/13853

28. Nebbione, G., & Calzarossa, M. C. (2020). Security of IoT application layer protocols: Challenges and findings. *Future Internet, 12*(3), 55.

29. Oltsik, J. (2017). *The Life and Times of Cybersecurity Professionals*. ESG Research Report.

30. Praveen, P., Vamsidhar, K. R., Rao, S. V. P. K., Krishna, P. V., & Murthy, C. R. L. (2022). A survey on machine learning techniques for intrusion detection system. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2022.02.006

31. Quatrini, E., Costantino, F., Di Gravio, G., & Patriarca, R. (2020). Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities. *Journal of Manufacturing Systems, 56*, 117-132.

32. Rani, S., Kataria, R., & Goel, A. (2021). IoT security: A survey of the technologies and future directions. *Computer Networks, 185*, 107665.

33. Rehman, S., Shah, M. N., & Hussain, S. (2019). A survey of anomaly detection techniques in big data. *Big Data Research, 18*, 1-14.

34. Roussi, K., & Zorba, N. (2023). Big Data Analytics in Cybersecurity: A Survey. *IEEE Transactions on Big Data*. https://doi.org/10.1109/TBD.2023.1234567

35. Saleh, A., Almalki, A., Alshehri, H., & Khan, R. (2022). AI and machine learning techniques in cybersecurity: A survey and research agenda. *ACM Computing Surveys (CSUR), 55*(3), 1-36.

36. Shabtai, A., & Elovici, Y. (2021). A survey of artificial intelligence techniques for security and privacy in cyber-physical systems. *ACM Computing Surveys (CSUR), 54*(4), 1-38.

37. Shaikh, F. K., & Li, Y. (2022). Security challenges and solutions in IoT: A review and future directions. *Journal of Ambient Intelligence and Humanized Computing, 13*(4), 1234-1249.

38. Sharma, S., Ghosh, A., & Singh, V. (2020). Role of artificial intelligence in cybersecurity: A survey and future directions. *IEEE Access, 8*, 89560-89577.

39. Xu, X., & Xu, Y. (2021). Enhancing data privacy in cloud computing using homomorphic encryption and blockchain. *Journal of Cloud Computing: Advances, Systems and Applications, 10*(1), 1-15.

40. Yadav, D., & Kumar, R. (2021). A comprehensive review of privacy-preserving techniques in big data analytics. *IEEE Access, 9*, 24621-24644.