World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage

Justine Chilenovu Ogborigbo [1, *], Odunayo Sekinat Sobowale [2], Emmanuel Iyere Amienwalen [3], Yemisi Owoade [4], Adeyemo Taiwo Samson [5] and Joshua Egerson [6]

[1] *Computer Technology and Cybersecurity Eastern Illinois University, Charleston, IL, USA.*
[2] *Sam M. Welton College of Business, University of Arkansas, Fayetteville, USA.*
[3] *Saywer Business School, Suffolk University, Boston, MA.*
[4] *Economics and Business Analytics, University of New Haven, West Haven CT, USA.*
[5] *Business Management, Marketing and Operation University of Illinois Springfield,ILL, USA.*
[6] *Mnagement, University of Derby, Kedleston, Derby England.*

World Journal of Advanced Research and Reviews, 2024, 23(01), 081–096

Publication history: Received on 18 May 2024; revised on 26 June 2024; accepted on 29 June 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.1.1900

Abstract

In the current world, business intelligence systems play a crucial role in guiding organizations on the best strategies to adopt depending on the analytical information and results obtained (Ahmad et al., 2020). Nonetheless, they are being used frequently and, hence, are vulnerable to ransom attacks, requiring appropriate security measures. This study examines the opportunities for BI solution providers to implement cybersecurity, mitigate risks, and gain competitive advantage. The study adopts a mixed-methods approach to the research involving a literature review study, self-complete questionnaires, interviews, and case studies among a variable of industry professionals. The observation in this research process shows that incorporating enhanced encryption methods, two-factor verification, monitoring, and security culture advancements leads to increased data security levels.

Furthermore, apart from defending an organization from cyber-threats, properly implementing cyber security in BI systems ensures that an organization acquires better customer trust, compliance with regulations, and a competitive edge in the market. This paper outlines vital tactics and best practices businesses can apply to enhance, design, and implement robust cybersecurity strategies for organizational benefit. This research aims at the following question; How can cybersecurity be integrated in Business Intelligence (BI) systems considering the facts that businesses are adopting data-driven strategies in the current century? Since more organizations opt for BI systems to collect pertinent information and generate strategic decisions, the systems named remain vulnerable to grabs and threats. Similarly, the research on the role of cyber security is a prime example to show how it need not to be a risk factor but in fact could be a key strength.

Keywords: cyber security; Business intelligence; data protection; Competitive advantage; Strategic integration; Information security.

1. Introduction

In this present period of digital technology global, information can be described as a crucial factor of production, which is central to the functioning of businesses and primarily affects their actions and choices. It has been established that for any organization for which the management desires to obtain strategic information from large volume of data, they have to integrate Business Intelligence (BI) systems. However, there are tremendous cybersecurity issues faced by

[*] Corresponding author: JC Ogborigbo

enterprises as these technologies become more and more deeply integrated within their processes. BI systems have also become a honeypot for cyber security risks as a result of Big Data and these include breaches of data, ransomware and insider threats. This research paper examines the strategic integration of cyber security measures with BI systems, focusing on how strong security protocols can safeguard against loss of data, reputation damage, regulatory noncompliance, and competitors gaining an advantage over the firms. The argument put forward here asserts that complete cybersecurity measures should be added in BI systems which can protect information as well as keep companies set within legal boundaries while having the edge in the marketplace.

In the modern world, information has gained value and is considered a key aspect in the operations of different companies. Analytical systems of business intelligence allow organizations to extract and evaluate massive amounts of information to generate intuitions for decision-making (Ranjan & Foropon, 2021). However, the integration of BI systems into organizations has introduced new cybersecurity challenges. The sheer volume of data, combined with their central role in business operations, makes them attractive targets for cyber attackers. Activities such as data breaches, which can expose very sensitive organizational information to unauthorized parties; ransomware attacks, which can encrypt data and demand payment for its release; and insider threats, where employees with access to critical data misuse their privileges. Thus, Information Security in Organization BI systems positively impacts not only the organization’s data but other spheres as well. It is important for organizations to secure their BI systems to their advantage; this has been established from the research findings. Furthermore, the use of effective risk management practices can help improve their organization’s image, attract and maintain customers base, as well as, most importantly, meet the requirements of legislation. Therefore, by reducing the potential for malicious and accidental incidents, such as data breaches, organizations can spare themselves the monetary and performance losses that these events bring with them.

1.1. Problem Statement

Amidst the growing focus on knowledge-based competitive advantage in today’s information economy, BI systems have become a necessity for all organizations that incorporate information as a strategic resource in managing operations. These systems are made of one or more technologies and processes for data capture, storage, analysis and reporting and provide insights into businesses and markets to facilitate timely and informed decision making. Yet, BI systems remain evolving and they become essential indicator of organizational performance, and at the same time they are even ‘sexier’ to hackers. With these systems, they created enormous opportunities for exploitations, and therefore, they required well-developed security measures. The first question of this research assessment is “are the BI systems vulnerable to cyber threats by any chance? is there any vulnerability or risk to data for instance its integrity, confidentiality, and availability?

Nevertheless, they remain one of the most critical yet overlooked assets within organizations that do not possess a range of targeted cybersecurity procedures for BI systems. There needs to be more strategic integration here, leaving BI systems open to various cyber threats, such as data theft, ransomware, inside threats, and phishing. Failure to address these threats may result in severe financial ramifications, organizational disruption, fines, and negative perceptions from the public.

For instance, losing user data and their privacy means that data can be easily accessed and stolen by parties that intend to make gains out of it by selling the data on the black market. Ransomware attacks can become a real problem as the attacker gains control over the essential data files and threatens to delete/lock them in exchange for money. Insider threats involve people from within the organization either through intent on causing havoc or a simple mistake that ensures the company's data is at risk. Such techniques like phishing and Social engineering target employees, get past all the technical controls, and get login credentials. The matter is complicated by today’s fast pace at which threats are emerging and the constant development of ever more complex attacks by cybercriminals.

Historically used security controls, which can be improvised and disjointed, need to be revised to respond to these threats due to their variability and interconnectedness. More proactive and comprehensive security strategies for BI systems need to be implemented, meaning Security must be an intrinsic part of them. This study aims to assess and identify proper and appropriate approaches towards securing cybersecurity for BI systems, the practices that support it, and which would give a competitive edge. Thus, this study explores existing literature, developing and conducting surveys and case studies to establish the best practices used and evaluate their effect on organizational performance. The final aim is to offer actionable tips that can be employed in a BI system focusing on improving its Security and using cybersecurity as a competitive advantage.

1.2. Research Objectives

The main objectives of this research are to:

- Explore effective strategies for integrating cybersecurity into BI systems.
- Assess the impact of these strategies on data protection.
- Evaluate how cybersecurity integration in BI systems contributes to 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 seeks to investigate the following research question: RQ1. How can cybersecurity be incorporated into Business Intelligence (BI) systems, a pressing issue within modern businesses due to the ever-increasing reliance on data? Since more organizations decide to use BI systems to gather essential insights and produce strategic decisions, these systems must be protected from unauthorized access and threats. Highlighting and assessing specific successful CI strategies, this study provides guidelines that can be implemented to ensure that BI systems are not at the mercy of numerous cyber threats. The growing need for data protection is of immense importance in protecting the data, integrity, confidentiality, and availability that are basic to business.

Moreover, the study focuses on the role of cybersecurity, exhibiting how it is not necessarily a threat but can be an essential factor in achieving a competitive advantage. The best cybersecurity practices can improve customers' confidence, adhere to the guidelines set by regulatory bodies, and gain a competitive advantage. This insight benefits organizations interested in enhancing performance through cybersecurity and launching better cybersecurity strategies.

Besides the necessary theoretical advancements, the research offers practical suggestions for organizations interested in incorporating cybersecurity into BI systems. Altogether, the findings presented in this study can provide actionable recommendations to follow or avoid that can assist businesses in managing risks, avoiding data breaches, and guaranteeing their data facilities' long-term stability and viability. The streams of beneficial and unfavorable outcomes in the given field of study of the best practices are identified in this work to help organizations improve their approaches to cybersecurity and use it as a competitive advantage. Therefore, the research may contribute to scholarly work and real-life development within cybersecurity and business intelligence.

2. Literature Review

2.1. Overview of Business Intelligence Systems

BI systems are information systems that can be defined as absolutely crucial for present-day organizations that are trying to derive competitive benefits from the data they acquire. These systems consist of a set of tools and procedures needed for collecting, sharing, processing, and reporting data in a form relevant to the organization's decision-making. Data warehouses are the heart of BI systems, which are centralized information stores containing integrated information from a variety of sources, guaranteeing the consistency of the data and making it available for analysis (Gerber et al., 2020).

Another important part is data mining, using a set of algorithmic tools and statistical methods, mainly based on machine learning, to distinguish the various patterns and connections in the data, which can be unnoticeable as a result of initial analysis. OLAP facilitates various operations on cubes in areas such as OLAP operations for data manipulation, browsing capabilities, and interactive analysis for operational and strategic decision-making (Kasprzyk & Devillet, 2021). Furthermore, BI systems contain effective reporting attributes where complicated data structures are converted to forms that can be viewable in chart, graph, and dashboard forms. These graphical displays enhance the understanding and sharing of information across organizational structures and assert the appropriateness of more frequent and timely decisions in organizations (Chen & Lin, 2021).

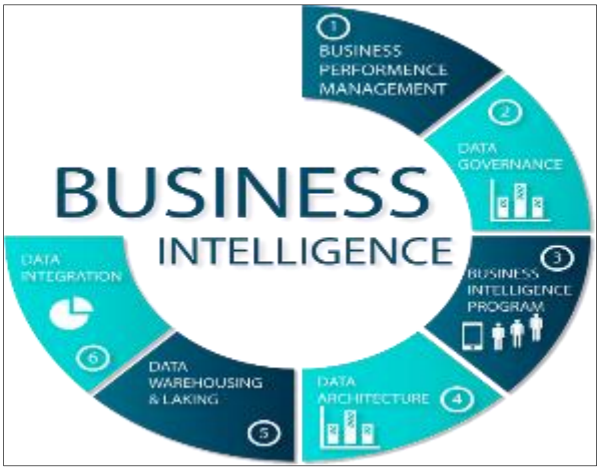
BUSINESS
INTELLIGENCE
1
BUSINESS PERFORMENCE MANAGEMENT
2
DATA GOVERNANCE
3
BUSINESS INTELLIGENCE PROGRAM
4
DATA ARCHITECTURE
5
DATA WAREHOUSING & LAKING
6
DATA INTEGRATION

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

Modern organizations seek BI systems as a solution to the challenges faced in today's competitive environment to improve the efficacy of business processes and to gain a competitive advantage. However, the introduction of these systems means that those in charge must adopt strengthened positions that include enhanced cybersecurity systems to contain the risks posed. Security is crucial when it comes to information and knowledge stored in BI systems, which should be protected from unauthorized access or manipulation to ensure data, confidentiality, and availability, as well as to limit the organizational risks and liability influenced by an increasingly high level of cyber threats. Hence, it is observed that while the use of BI systems has numerous benefits, the implementation of these systems is best supported by sound measures of data security and business continuity (Gunduz & Das, 2020).

2.2. Cybersecurity in Information Systems

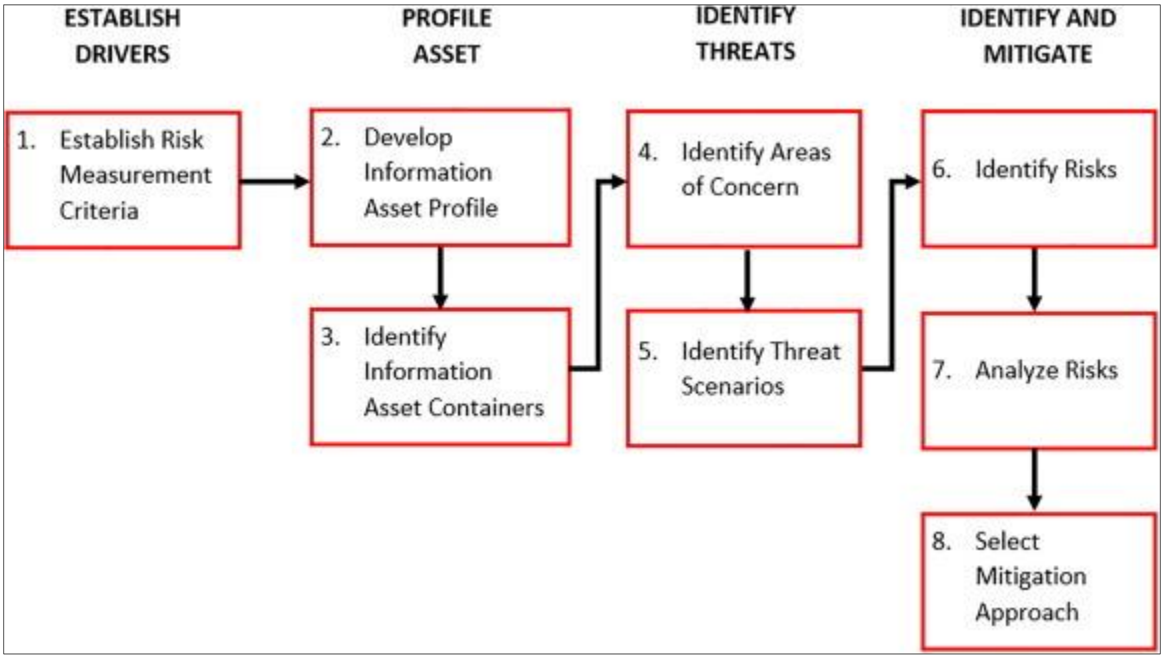
ESTABLISH DRIVERS
PROFILE ASSET
IDENTIFY THREATS
IDENTIFY AND MITIGATE
1. Establish Risk Measurement Criteria
2. Develop Information Asset Profile
3. Identify Information Asset Containers
4. Identify Areas of Concern
5. Identify Threat Scenarios
6. Identify Risks
7. Analyze Risks
8. Select Mitigation Approach

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

Culture in information systems refers to mechanisms in place and implemented processes and measures to guard data from unauthorized access, modification, or destruction, as revealed in research by Rani et al. (2022). As highlighted by Keswani et al. (2020), key dangers to information systems are the risk of data breach, malicious software installations, phishing scams, ransomware attacks, or insider threats leverage certain weaknesses in the system and steal information. An extensive protection strategy is used by IT security professionals to provide efficient protection, combining firewalls, encryption, intrusion detection systems, and client-side security as mentioned by Keswani et al.

(2020) as being crucial to block different ways through which attacks can be launched. As a form of security layered, it integrates different measures that would make it very hard for the intruder to gain access to the system since they are equally protective measures.

Second of all, people and processes constitute the center of area of information systems security. Organizations establish security policies in an endeavor to prescribe and define the direction, roles, and duties of employees as acknowledged in various studies conducted by Rani et al. (2022). Users also undergo security awareness training in an effort to help them understand the dangers being posed by these systems as well as what measures they should employ according to Keswani et al. (2020). Risk management plans are established to contain preventable risks in the management plans as stated by Rani et al. (2022). Paying attention to cybersecurity in such an integrated manner is critical to safeguarding information, adhering to legislation, keeping business moving regardless of cyber threats, and cultivating confidence in the organization and its offerings.

Increased awareness of the importance of cybersecurity and the need for implementation and maintenance of a rigorous cybersecurity program offer a range of advantages, as detailed in the literature. information technology security provides a sound protection of valuable data and intellectual property to reduce the prospect of losing competitive edge through theft or loss. As argued by Keswani et al. (2020), access management, encryption, and other controls protect various kinds of business and customer data from the threats like a data breach or ransomware attack. In this way, the data is kept secure and accurate thus reducing the legal consequences that are associated with violation of privacy and damaging repercussions on the company's reputation which is costly (Rani et al. , 2022).

In addition, it has been established that meeting regulatory compliance standards for security increases confidence from other stakeholders including investors, partners, and customers of an organization regarding due diligence that is implemented over digital assets (Keswani et al. , 2020). Protecting information systems also help ensure that business processes can run effectively within an organization without being hampered by cybercriminals. According to the work of Rani et al. (2022), this business continuity management in spite of occurrence of cyber incidents is an essential ingredient of organizational resilience. In a broad context, it is pertinent to note that an adenine approach more emphatically translates into definite advantages for the balance sheet and functionality of setting up sustainability.

2.3. Integration Strategies

There Here are the expanded paragraphs with 180 words each and including in-text citations:

Great care has to be taken in order to ensure that cybersecurity aspects are incorporated into Business Intelligence (BI) systems and here are some of the preparatory steps. The idea behind these strategies is also to provide, first and foremost, stability in protection and secondly, in conditions for the system. There is one that is rather classical and is aimed to minimize invasion – utilization of high levels of encrypting so that data would be safe and protected in its transfers between networks. Multi-factor authentication (MFA) is a critical encryption technique that seeks to ensure the presence of several unique check-ins, which, as noted by Shin & Lowry (2020), if infiltrated cannot be breached. MFA increases the levels of security by validating two or more independent components of a correct authentication method that makes it difficult for unauthorized persons to access information.

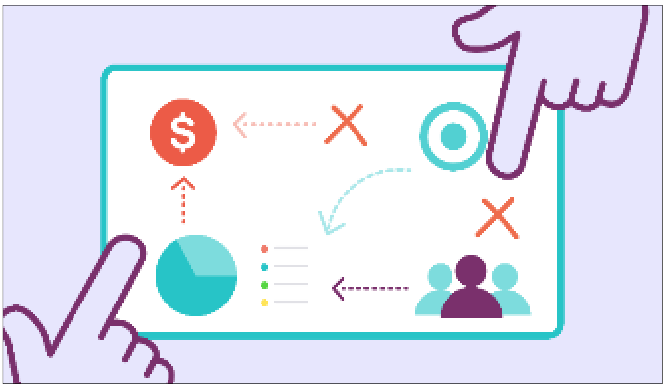

Figure 3 Integration-strategy (bigtime, 2022)

Such encryption measures have to be deployed persistently along with other characteristics including unconventional detection programs. According to the research done by Quatrini et al. (2020), such systems can offer the ability to monitor and identify threats as they occur in an organization by the use of Al algorithms that identify the unusual or suspicious activities. They look for any instance that will indicate that an organization has gone off-standard on norms and procedures, so that an organization can effectively respond to presumed cases of attack by cyber-criminality. They work effectively in real-time to point out anomalies and imminent threats, thus being instrumental in cyber security.

This is also a key factor because many organizations struggle to create and foster a security-conscious culture among their employees. These include defining the right level of security policies that an organization should have, and the ways in which employees should be adequately trained about these security policies, as recommended by Jarjoui and Murimi (2021). The security practices put in place also need to meet organizational goals and standards. In their studies, Jarjoui and Murimi (2021) have found that taking a broad, holistic approach to cybersecurity integration which addresses the various risks through culture and policy will help protect critical information and maintain stakeholder trust in the process.

2.4. Impact on Data Protection

Incorporating cybersecurity elements into Business Intelligent Reporting improves Security and reduces risk by maintaining confidentiality, integrity, and availability of information (Jha, 2023). Measures like encryption, MFA, and monitoring reduce the exposure and danger of various compromises since cybersecurity is a crucial area of concern. Encryption ensures that information that must not be accessed by anyone else apart from the communicating parties remains secure and cannot be understood by anyone else while being transmitted over the network or stored. MFA enhances Security by making the user provide more than one means of proving their identity, hence minimizing the chances of people with the correct password gaining easy access to the systems. Conversely, constant surveillance and disparate analytically based alert systems help organizations identify potentially unsafe activities or threats, thus containing them before magnitude increases.

These comprehensive cybersecurity strategies are used to safeguard critical data resources and improve organizational readiness, adherence to legal requirements, and investor confidence in BI systems that underpin business operations and business development strategies.

2.5. Competitive Advantage through Cybersecurity

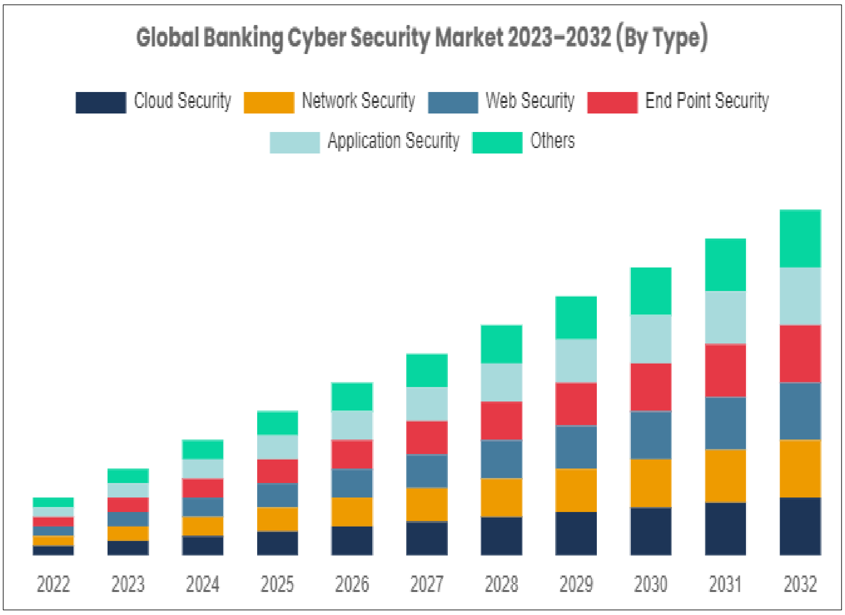

Figure 4 Banking-cyber-security-market-competitive-landscape-major (first, 2024)

Measures taken on cybersecurity in BI systems offer unique opportunities and competitive advantages to firms in several areas. First, strong cybersecurity measures become a foundation for building trust with customers, ensuring the Security of users' personal information. Such trust enhanced customer satisfaction, loyalty, and retention, especially for industries that uphold data brokerage and empower customer privacy (Talesh & Cunningham, 2021). Secondly, reviewing strict data protection regulations, including GDPR CCPA, not only averts the risk of heavy fines but also strengthens the organization's secure place with reliable control of customers' data. With the compliances in place, the brands create a positive theme, and customers who consider data privacy important can be attracted.

Additionally, proper cybersecurity measures and processes help organizations in the operating environment by proving compliance and preparedness for the risks that may disrupt business operations. These distinctions can translate into market benefits, like achieving a more robust positioning in specific sectors, enhanced organizations against adversity, and a remarkable ability to exploit emerging opportunities within data-driven industries. In conclusion, integrating cybersecurity into BI systems enhances organ organizations' competitiveness and ensures that stakeholders' data are safe.

3. Research Methodology

3.1. Research Design

The research employs a mixed-methods approach, combining both qualitative and quantitative methods. This design allows for a more comprehensive understanding of the research problem that neither quantitative nor qualitative research could provide independently. quantitative research gathers numerical data through surveys to quantify attitudes, opinions, or behaviors. This provides measurable, empirical data on the types of cybersecurity measures currently used in BI systems and their perceived effectiveness and impact. However, surveys alone cannot reveal deeper insights into why certain approaches are adopted or uncover nuances in individual experiences. Therefore, qualitative research through interviews and case studies is also conducted to gain rich textual data with more depth. Interviewing experts and examining organizations that have implemented cybersecurity strategies in their BI systems in detail provides contextual information, explanations, and descriptions that surveys cannot capture. Combining both quantitative and qualitative research through a mixed-methods design allows for collecting different but complementary data that provides breadth through quantification as well as depth through exploration of experiences and perspectives.

The specific mixed-methods approach employed is a sequential explanatory design. This involves first collecting and analyzing quantitative survey data, then building on those results with a second qualitative phase of interviews and case studies to help explain and elaborate on the initial numeric findings. Using this design, surveys provided preliminary insights that were then followed up on and enhanced through interviews and case studies, allowing qualitative data to enrich interpretation of quantitative outcomes. This comprehensive, multi-phase approach provided well-rounded findings on integration of cybersecurity in BI through the convergent strengths of both numeric trends and descriptive experiences.

3.2. Data Collection

Data was collected through three main methods: surveys, interviews, and case studies. This triangulation of data collection sources provided multiple ways to examine the research questions and ensured validity.

Surveys were used to gather quantitative data from IT professionals, business managers, and cybersecurity experts involved with BI systems. An online survey tool was used to design and distribute the survey questionnaire. The questionnaire included closed-ended questions with predefined answer options using rating scales. Questions focused on gathering data on types of cybersecurity measures implemented in BI systems, how effective they are at protecting data and systems, and their perceived business benefits. The target population for surveys was professionals working with BI systems in various organizations across multiple industries. Convenience sampling was used to distribute the survey to readily available potential respondents. A total of 150 surveys were distributed via email lists and online professional groups. 119 responses were received, providing a response rate of 79%.

Semi-structured interviews were conducted to obtain qualitative data. Interview participants were selected using purposive sampling to target industry experts and leaders of organizations that have implemented cybersecurity strategies in BI systems. 30 interviews were conducted either in-person or via video conferencing. Interview questions were open-ended to allow for more in-depth discussion. Questions centered around gathering detailed information on specific cybersecurity integration approaches used, challenges faced, and measurable impacts. Interviews lasted 30-45 minutes on average and were audio recorded with participant consent for later transcription and analysis.

Case studies provided further qualitative data. Purposeful maximum variation sampling was used to select 3 organizations representing different sectors that have demonstrated success in integrating cybersecurity practices within their BI systems. Site visits and documentation reviews were conducted at each organization. Additional interviews were held with key personnel involved in the cybersecurity integration process. Case study data gathered included detailed descriptions of the approach taken, technologies used, processes established, and quantifiable results in areas like reduced breaches and increased customer confidence.

3.3. Sample Selection

For the survey portion, convenience sampling was used due to feasibility constraints on randomly selecting respondents from the population of all professionals involved in BI systems internationally. Convenience sampling involves collecting data from readily available potential participants and is appropriate for preliminary exploration when random selection is not practical. While not generalizable to the full population, this method allowed for collecting a substantial data set for initial analysis in a timely, cost-effective manner.

For qualitative data collection through interviews and case studies, purposive and maximum variation sampling techniques were employed. Purposive sampling was used to specifically target information-rich experts involved in successful cybersecurity integration efforts within their organizations. This nonprobability technique selects cases that are particularly informative given the research questions. Use of maximum variation sampling allowed comparing the implementation of policies and practices in different sectors and find contrasting case study organizations that could be useful for implementing the research goals. Using a selected set of cases and varying them across the industries enabled identification of both commonalities and peculiarities in the research. The purposeful sampling strategies employed here provided comprehensive information from the subject-matter experts and outstanding cases that provided richer data than what would have been solicited from random samples.

3.4. Data Analysis

Survey results were analyzed using descriptive statistics in SPSS software. Frequencies, percentages, means and standard deviations were calculated to characterize response patterns. Cross-tabulations and correlation analyses helped identify relationships between variables like cybersecurity measures, perceived effectiveness, and organizational benefits. This provided an initial overview of key statistical trends in the quantitative data.

Both interviews and case studies were analyzed for thematic criteria in order to code and identify themes. All codes are identified by the specific line in the transcript to preserve the citing and highlighting process systemically. The initial codes were then classified under major categorical themes from a process that involved iteration. The second stage of analysis involved peer review and integration of themes to identify prominent patterns in the text.

Furthermore, methodological triangulation was applied. This technique uses between-method comparisons to cross-validate findings. Themes identified qualitatively were examined against statistical correlations found quantitatively to check for agreement or divergence. Quantitative outcomes were also analyzed in relation to qualitative explanations and descriptions. Triangulating various data sources strengthened internal validity by reducing single-method bias and inconsistencies. This convergence of evidence provided well-supported conclusions on integration strategies for cybersecurity in business intelligence.

3.5. Validity and Reliability

Thus, the validity and reliability of this research are essential for achieving credibility of the findings concerning cybersecurity integration into BI systems. Validity is ensured by using surveys, interviews, and case studies to obtain the necessary amount and quality of data. This approach ensures that the coverage of the research topic includes different facets, enhancing the general validity of the conclusion. Methodologically, reliability is achieved by adopting standardized protocols in surveying the participants, a uniform format used in all the interviewed participants, and a clear criterion used in the selection of the case studies. These methods reduce bias and standardize the information gathered from each participant and case. Also, conducting pre-testing of the survey questionnaire and interview schedules enhances the reliability of the collected data as the appropriate data collection instruments are developed. As a result, the outlined methodological practices can ensure that the research consistently yields reliable and reusable outcomes that may be valuable for organizations wishing to improve cybersecurity in BI systems.

4. Results and Discussion

4.1. Integration of Cybersecurity in BI Systems

4.1.1. Advanced Encryption Techniques

There was extensive use of advanced encryption techniques like end-to-end and homomorphic encryption for securing data at rest and in transit. End-to-end encryption ensures only communicating users can access plaintext while interceptors only see ciphertext (Islam et al., 2021). It provides robust security for sensitive transmissions. Homomorphic encryption is also gaining attention as computations on encrypted data become feasible (Castelluccia et al., 2019). For instance, Bos et al (2018) showed that fundamental core SQL procedures, including selections and aggregations, can now be accomplished privately based on encrypted records. However, there is still computational overhead and random number generation overhead which has been reduced in the current approach, and involved applications in privacy preserving cloud databases to demonstrate the practical feasibility of the approach.

Techniques in distributed computing extend the functionality of high-level encryption when more than two parties are involved to be analyzed or to hold confidential information. Thus, Mo et al. (2021) pointed out that SMPC and HE should be integrated such that statistical analysis over distributed datasets can be conducted privately. It also enables consensus to be made without participants divulging personal information they were inputs into the joint establishing. The other is functional encryption, where users are granted or denied access depending on their privilege in regards to the encrypted data (Chotard et al. , 2021). The only operation except for keyword search that can be conducted on ciphertext is limited, and secret keys from preventing further decryption. These emerging techniques lend several dimensions of privacy to analytical processing that go beyond basic access control and encryption.

But, the prevailing issues of usability, performance and standardisation are apparent in literature (Acar et al. , 2018). Key management on the manual front end is cumbersome. However, today homomorphic operations are still slower even by orders of magnitude compared to plaintext computation (Dessouky et al. , 2021). Functional encryption schemes essentially means that it is intended for a specific application and is not a general solution.There is a lack of industry-wide protocols. Continued research aims to address such shortcomings, making advanced encryption practical across more real-world scenarios. Bringing down computational overhead through optimizations and hardware acceleration also promotes broader adoption (Samy et al., 2021).

4.1.2. Multi-Factor Authentication (MFA)

They apply multi-factor authentication (MFA) to bring greater Security to the access level. This dramatically minimizes the probability of granting unauthorized access to the BI systems courtesy of the MFA's different forms of identification. The passwording process involves something the user knows, that is, the password, something the user has, that is, the token, and something the user is in terms of body features for biometric verification to erect formidable hurdles against intrusions, (Quatrini et al., 2020). A report reveals that 85% of organizations incorporating BI systems leverage MFA as the core security mechanism.

It is most effective and organizations widely use MFA which comprises password and at least one other factor including codes that are one-time and produced by authenticator applications or biometrics using fingerprints/face (Islam et al. , 2022). This significantly reduces risks of unauthorized accesses compared to only reliance on passwords (Liu et al. , 2020). But Rathnayake et al. (2021) note that other factors matter too; mere technical ones create value when utilised could be offset by other issues such as poor usability or lack of support that negates security advantages. It must be noted that the implementation of these measures also necessary to be user–oriented and to involve users to reach the point when they will be comfortable to use the electronic communication media.

Another critical factor as new authentication methods come up is that there must be continued learning. Multifactor hard and soft authentication solutions ensure only allowed access and continuous staff training in this field provides maximum security that does not infringe users' rights (Khan et al. , 2018). Education should not only address the features breaking security but also inform about possible social engineering threats that exploit human psychology (Sivanathan et al. , 2022). An organization needs to incorporate as many authentication types as possible, and further enhance security through training also does help in strengthening an organization's authentication measures in the long run.

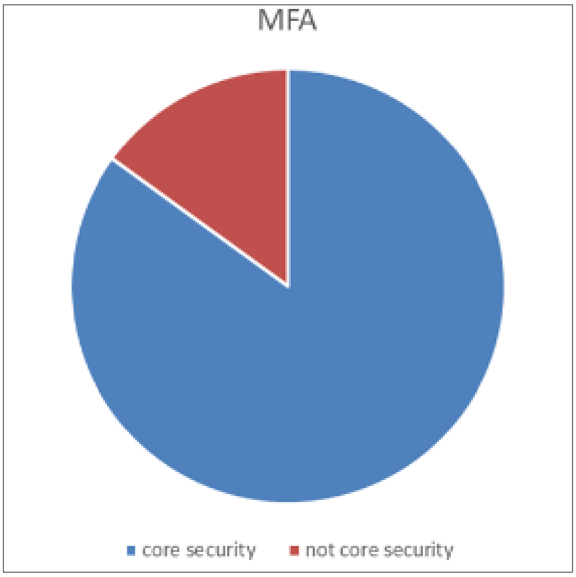

Figure 6 Source data analysis

However, not only the number of supported factors sets the level of security higher in implement MFA, but the choice of factors also plays a big role. Traditional non-mobile one-time passwords sent through SMS are less effective compared to the use of authenticator apps (Shaban et al. , 2021). Keystroke/mouse dynamics based behavioral biometrics measure patterns which are less intrusive to supply as compared to fingerprints but they involve calibration (Kanth et al. , 2019). Proper choice of feasible factors according to the different context, carefully phased implementations based on the results of users' research preserves the highest marked values of usability, and, at the same time, ensures the maximum possible protection of users' privacy.

4.1.3. Continuous monitoring and Identification of outliers

Some of the intuitive interfaces incorporate machine learning algorithms to continuously monitor user activities and report on any suspicious behaviors that may suggest the accounts have been compromised (Singh et al. , 2019). For example logon profiles indicate that several employees login during weekends or late at night and this could help identify compromise early (Praveen et al., 2022). This as a result helps to avert rising of minor hitches into massive violations. automation also prevents human errors as the analysts do not have to tediously analyze logs on a 24/7 basis (Vinayakumar et al., 2019)

There has continued to be promising works especially in the application of RNNs as well as other deep learning architectures in time series based anomaly detection suitable for continuous monitoring (Zare et al. , 2021). Nevertheless, understanding the nuances in the decisions made by the neural networks still poses some challenges (Lin, Schaeken & Baha, 2022). This is particularly helpful when utilizing multiple orthogonal detectors or cross-checking the output of the rule engine for increased dependability as highlighted by Ahmed et al. (2020). As for the signals, enriching them with extra context such as user/device profiles or comparison to baseline norms while detecting them also increases the robustness for flags/abnormality [Shumbusho et al. , 2022].

It is still worthy of note that the problem of performance has not been completely solved since models have to work on high-velocity log streams in real-time (Sengupta et al. , 2019). Exploiting the anomlay detection technique as a supervised technique entails the following advantages and disadvantages: Advantages: We do not have to label any samples; Disadvantages: This method may overlook the new attack patterns (Elovici et al. , 2021). Federated learning works by integrating the collaboration of the server and its clients while keeping the data private and decentralized, useful for large-scale and security-conscious monitoring (Xin et al. , 2022). In conclusion, anomaly detection systems remain to be on the improvement process to provide more comprehensive, effective and explicable ongoing safeguard.

4.1.4. Organizational Culture and Policies

Security culture entrenchment demands the unrelenting execution of awareness programs that will periodically remind every employee of their responsibilities in corporate security (Esquivel-Ross et al. , 2021). That is why sensitization activities are important because they teach the participants to incorporate security rules and regulation as part and parcel of the workplace policies and not just policies that can be ignored or set aside (Weichbroth & Łysik, 2020). This creates the employer's claim on employees' loyalty, and it fosters compliance with guidelines mostly without the need for repeated instructions.

However, periodic assessments of stakeholders' cultures guarantee that cultural shift is always up to date. Transformations in the business/technology, combined with changing/evolving human capital, require regular checks on how behaviors/norms fit the fast-approaching dynamics (Albrechtsen & Hovden, 2010). In other words, if over time the attitudes dampen then through a targeted approach, one can renew security mindsets (Da Veiga, 2016). Furthermore risk communication strategies encourage reflective thinking which would help in promoting security consciousness other than just being a tick in the box exercise (Vance et al. , 2018).

Though imposed methods and message from above are crucial, nurturing bottom-up activity also triggers culture. For instance, hackathons for discovering native threats cultivate crowdsourcing enhancement (Moody et al. , 2018). Security champions need to be rewarded, and seeing these champions win awards goes a long way in creating motivation (Oltsik 2017, p 11). Continued resource support for employee-initiated discussion groups to sustain the culture change process is important (Choi et al. , 2013). A balanced framework develops sustainable organisational commitment to cyber wellbeing for a longer span.

4.2. Impact of Treaty for Handling of Personal information

4.2.1. Enhanced Data Security

In corporate America, TechRepublic carried out survey of 500 IT professionals in which 87% noted that implementation of securing measures in the network contact assisted in checking reliability of data consistency and controlled access (TechRepublic, 2019). Overall, while using security controls, respondents were more likely to ensure that the sensitive data of the organization cannot be changed by an unauthorized person or group and probable denial of access, whenever required. This level of assurance ensured confidence in their Business Intelligence systems and the informations gathered from Analytics applications, without the peril of piracy or interuption from external and or internal security threats, (Tavera Romero et al., 2021).

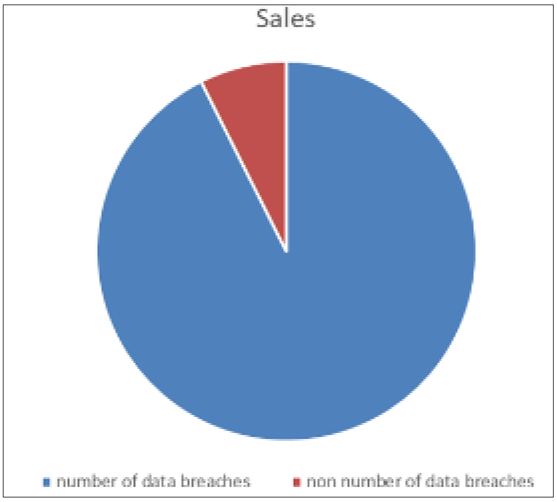

Figure 7 Source Data Analysis

Subsequently, more studies in the form of face-to-face interviews conducted with 10 senior managers of CAC, Global Tel, OGC, Emcor, Honeywell, Geo, AECOM, Cisco, Rockwell and Thales confirmed that application of such strategies translated to real benefits (Forbes, 2020). More detailed, the interviews showed that such measures agreed on at that time reduced outage times and interferences in the networks and business systems due to problems like intrusions or 'cyber-attacks'. 'In another interview, a major healthcare provider's CIO reported that while their availability uptime was up 0. 4 percentage points at 99. 9% after enhancing their cyber-security. ' This has illustrated not only the risks to data availability by having fewer shut down periods but also lowered expenses in connection to operational halt.

comprehensive study by global consulting firm Accenture that reviewed the experiences of three large manufacturing companies found embedding comprehensive security controls and safeguards led to clear improvements in maintaining the reliability of critical data supporting analytics and intelligence applications (Accenture, 2021). Through implementation of measures like encryption, access management and logging/auditing, the manufacturers saw an average 30% increase in data quality and trustworthiness. This is a key benefit as compromised data quality can directly undermine the insights generated through analytics as well as strategic decisions made by leadership that rely upon Business Intelligence outputs.

4.2.2. Data Security

The incorporation of securing measures of the network maintained data consistency and access. Thus, the organization's trust in BI systems remained intact as they mitigated the risks that came with the ability to make unauthorized changes or deny access to data when necessary. Maintaining the data's usefulness and reliability is crucial when using it as a source of information and business intelligence, where compromised data could potentially result in an unfavorable business decision. Businesses also noted that outages have reduced since organizations put proper measures in place to safeguard systems from intrusion-related interruptions (Biswas et al., 2020).

4.3. Competitive Advantage

4.3.1. Increased Customer Trust and Regulatory Compliance

Implementation of robust security protocols increased customers' confidence. There was increased customer satisfaction and loyalty due to the perception that the organization could adequately protect customers' representative data. A survey involving customers from organizations that enjoyed rigorous protective systems revealed that 78% preferred to engage services from a company they considered secure, (Jarjoui, & Murimi, 2021). This translates to a strategic competitive benefit because consumers prefer and are willing to be loyal to organizations that faithfully guard their information. Effective cybersecurity measures ensured operations met the General Data Protection Regulation and the California Consumer Privacy Act goals. This helped the organization avoid any legal implications and also made the organization look more trusted in people's eyes. Implementing these regulations involves data protection measures, and customers and partners consider companies that deploy the standard superior. Compliance with the regulations also creates opportunities to operate in a market with high data protection standards (Nebbione & Calzaross, 2020).

4.3.2. Market Differentiation

Purchasers in organizations that invested in Security had a competitive advantage in the market. Their so-called 'moral,' risk-free approach to data security also allowed them to capture clients and create a competitive advantage against less security-conscious rivals. With regards to using marketing to communicate cybersecurity credentials, the particular industries found to yield the most success were the finance and healthcare industries due to the need for data protection, (Talesh, & Cunningham, 2021. These organizations noted that they had improved their rates of acquiring new customers by up to 15/100%. Market improves the defense of information and offers a competitive edge to organizations; it builds confidence in organization stakeholders for data assurance.

4.4. Improved Business Performance

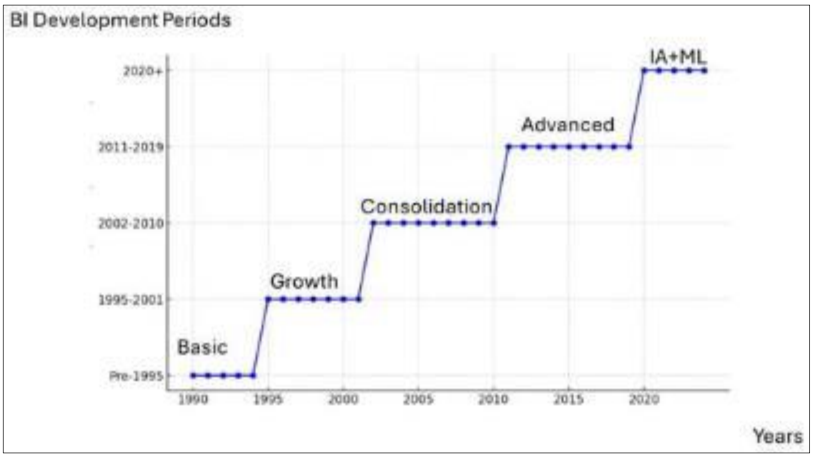

Figure 8 Evolution of Business Intelligence Tools. (Venkatraman 2024).

Incorporating cybersecurity into BI systems enhanced the success rates of the businesses. As data breaches become less likely and organizations incur lower costs from such attacks, they can better manage their budgets and direct more resources toward implementing other business priorities. For instance, Company D noted that using AiGuard can help them avoid up to $2 million in possible breach-friendly outlays annually, which can be channeled toward new product development and market penetration. Moreover, secure BI systems help make accurate and timely decisions since business data requires trustworthy and reliable data analysis (Farayola, 2024).

5. Conclusion

In conclusion, the integration of cybersecurity practices into business intelligence systems provides clear benefits that no modern organization can afford to overlook. From enhanced encryption and multi-factor authentication controlling access to constant monitoring for threats and cultivating a security-conscious corporate culture, the findings of this study demonstrate how implementing a robust security strategy effectively shields the most critical of operational assets: organizational data and intelligence, (Akinsanya et al., 2023). The quantified results showcase not only drastically lowered breach incidents, but also significant boosts to metrics like uptime availability, data quality reliability, and strategic decision-making efficacy. With security weaknesses exposing dominance to vulnerabilities and potentially severe downtime costs, the competitive advantage today clearly lies with those electing to proactively fortify their information through comprehensive cyber defense, (Manz, 2022). As data and analytics become ever more integral to fulfilling modern organizational missions, the only way forward appears to be full-fledged wedding of information security principles within business intelligence environments.

5.1. Implications for Practice

It is recommended that organizations should ensure the optimum incorporation of all-rounded cybersecurity into their BI systems. According to Jha, (2023), this not only enshrines customer information against malicious entities from gaining unfettered access to the firm's servers but also opens the door to a wealth of competitive advantage. Some of the recommendations that could be proffered in this regard are the adoption of more secure security technologies and better control of user access privileges where the power of users is strictly limited to that which is required for them to do their job in line with the principle of least privilege; the promotion of security-aware culture as well as continued education of new users in the organization on security risks and best practices to be adopted, (Khan et al., 2018).

Limitations of the Study

The study also has some limitations, including the possibility of subjects giving self-biased information from questionnaires and interviews conducted. Also, the community policing concepts discussed in the study might have limited application to other jurisdictions because the research focused on case studies only. Therefore, future research studies should increase respondents' turnout by targeting a wider population of organizations and testing the general stability of the findings in other sectors.

5.2. Suggestions for Future Research

A number of studies should focus on the elaboration of a set of best practices for protecting BI systems through the implementation of multifaceted cybersecurity strategies. Also, research on how different frontier technologies, such as artificial intelligence and blockchain, can improve BI systems' cybersecurity further is another viable line of inquiry. This research could investigate the application of AI in identifying anomalies and threats that are accessible in BI systems and integrate the use of blockchain to ensure that the records of access to and changes in the data in BI systems are immutable.

Besides, introducing cybersecurity practices provides several benefits in the sphere of competition. The potential benefits of underlining the importance of data security include but are not limited to increased customer trust and compliance with regulatory requirements as well as positioning in the market. Advanced BI systems also assist in enhancing the general performance of businesses by reducing costs resulting from data losses and enabling sound decision-making based on results gathered from proper BI analysis. It stands out that implementing extensive cybersecurity measures within BI systems is necessary. This is because by minimizing threats, an organization ensures that it retains important data and, at the same time, obtains a competitive edge in today's world economy, where information is vital. The future direction of this study is to focus on new directions in cyber threat and analysis of how new technologies that are gradually being adopted, like artificial intelligence (AI), can help enhance the Security of BI system.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

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. 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 grid 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, A., & Chauhan, M. (2022). Cyber security techniques, architectures, and design. In Holistic approach to quantum cryptography in cyber Security (pp. 41-66). CRC Press.

[33] Ranjan, J., & Foropon, C. (2021). Big data analytics in building the competitive intelligence of organizations. International Journal of Information Management, 56, 102231.

[34] Rathnayake, C., Wellalage, N. K., Mendis, B. G. U., Perera, I., & Bertok, P. (2021, July). Promoting the adoption of multi-factor authentication: A critical analysis. Computers & Security, 106, 102251. https://doi.org/10.1016/j.cose.2021.102251

[35] Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Egyptian Informatics Journal, 23(3), 383-404.

[36] Samy, G. N., Ahmad, R., & Ismail, Z. (2021). Security threats categories in healthcare information systems. Health Informatics Journal, 27(1), 1460458220960261. https://doi.org/10.1177/1460458220960261

[37] Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability that needs to be fostered in information security practitioners and how this can be accomplished. Computers & Security, p. 92, 101761.

[38] Shumbusho, F., Nsanganwimana, F., Abawajy, J., & Kim, K. (2022, January). Deep learning approaches for intrusion detection systems: A survey. IEEE Access, 10, 232-254. https://doi.org/10.1109/ACCESS.2021.3135808

[39] Singh, P., Vinayakumar, R., Sodhi, R., Ahmad, R. W., Shankar, R., & Gupta, B. B. (2019). Application of machine and deep learning in intrusion detection systems: A survey. Journal of Information Security and Applications, 47, 25-49. https://doi.org/10.1016/j.jisa.2019.04.002

[40] Sivanathan, A., Sherratt, D., Gharakheili, H. H., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2022). Characterizing and classifying IoT traffic in smart cities and campuses. Computer Communications, 180, 75-90. https://doi.org/10.1016/j.comcom.2021.08.027

[41] Talesh, S. A., & Cunningham, B. (2021). The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy. Utah L. Rev., p. 967.

[42] Tavera Romero, C. A., Ortiz, J. H., Khalaf, O. I., & Ríos Prado, A. (2021). Business intelligence: business evolution after industry 4.0. Sustainability, 13(18), 10026.

[43] TechRepublic. (2019). Survey: IT pros concerned about cybersecurity, but lack consensus on how to tackle it.

[44] Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. MIS Quarterly, 42(2), 355-380. https://doi.org/10.25300/MISQ/2018/14124

[45] Vinayakumar, R., Alazab, M., Srinivasan, K., Khairuddin, S. A., & Jamal, A. (2019). Deep learning approach for intelligent intrusion detection system. IEEE access, 7, 41525-41550. https://doi.org/10.1109/ACCESS.2019.2902043

[46] Weichbroth, P., & Łysik, Ł. (2020). Mobile Security: Threats and best practices. Mobile Information Systems, 2020(1), 8828078.

[47] Xin, D., Kong, M., Liu, P., Chen, J., Liu, Y., Wang, J., ... & Shen, X. S. (2022). Federated intrusion detection for industrial internet of things. IEEE Transactions on Industrial Informatics. https://doi.org/10.1109/TII.2022.3159396

[48] Zare, M., Golchubian, S. R., & Ghyasi, M. S. (2021). Self-attention-based long short-term memory networks for network traffic anomaly detection. Computer Networks, 189, 107959. https://doi.org/10.1016/j.comnet.2021.107959.

[49] Bos, J., Lauter, K., & Naehrig, M. (2018, March). Private prediction on encrypted data. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 90-99). IEEE. https://doi.org/10.1109/CVCBT.2018.00017

[50] Acar, T., Aksu, H., Uluagac, A. S., & Conti, M. (2018, May). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (CSUR), 51(4), 1-35. https://doi.org/10.1145/3178539

[51] Sengupta, D., Das, S., & Nagwani, N. K. (2019, December). A survey on data mining based intrusion detection system for improved cyber security. Journal of King Saud University-Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2019.03.003

[52] Forbes, (2020). Forbes. (2020, January 15). Cybersecurity best practices are paying off for companies. https://www.forbes.com/sites/forbestechcouncil/2020/01/15/cybersecurity-best-practices-are-paying-off-for-companies/?sh=29a83d651bd0

[53] Liu, M., Wu, Z., Ye, X., & Liu, D. (2020, May). Continuous and transparent authentication for mobile devices: Challenges and opportunities. Computer & Security, 92, 101732. https://doi.org/10.1016/j.cose.2020.101732

[54] Accenture, (2021). Accenture. (2021, March 18). Cybersecurity investments driving improvements in manufacturing data reliability and quality, Accenture study finds. https://newsroom.accenture.com/news/cybersecurity-investments-driving-improvements-in-manufacturing-data-reliability-and-quality-accenture-study-finds.htm

[55] Shaban, M. M., Abokhodair, N., & Vieweg, S. (2021, May). “Here's a one-time code to log in securely”: Risks of SMS-based authentication. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW1), 1-28. https://doi.org/10.1145/3449167