International Journal Software Engineering and Computer Science (IJSECS) 3 (3), **2023, 386-396**
Published Online December 2023 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN : 2776-4869, E-ISSN : 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v3i3.1816.

Edge of Enterprise Architecture in Addressing Cyber Security Threats and Business Risks

Loso Judijanto
Public Policy Research, IPOSS Jakarta, Indonesia.
Email: losojudijantobumn@gmail.com

Djarot Hindarto *
Informatics Study Program, Faculty of Communication and Informatics Technology, Universitas Nasional, City of South Jakarta, Special Capital Region of Jakarta, Indonesia.
E-mail: djarot.hindarto@civitas.unas.ac.id

Sentot Imam Wahjono
Management Study Program, Faculty of Economics and Business, Universitas Muhammadiyah Surabaya, Surabaya City, East Java Province, Indonesia.
E-mail: sentot.imamw@fe.um-surabaya.ac.id

Djunarto
Postgraduate Master of Management, Faculty of Economics, Universitas Jayabaya, East Jakarta City, Special Capital Region of Jakarta, Indonesia.
E-mail: djunartobeyzena@gmail.com

Received: 16 November 2023; Accepted: 28 November 2023; Published: 20 December 2023.

Abstract: Enterprise Architecture plays a critical role in reducing business risks holistically and ensuring a company's resilience to cyber security threats. This abstract emphasizes the significance of Enterprise Architecture in contemporary organizational structures and its influence on these matters, particularly at a time when cybersecurity threats are becoming more prevalent in the global business arena. By integrating Human Resources, Governance Frameworks, Technology, and Processes, Enterprise Architecture offers a holistic perspective of the Information Technology environment within an organization. By means of a methodical governance framework, Enterprise Architecture conducts comprehensive examinations of interdependencies among components, detects susceptibilities, and establishes robust groundwork for enhanced threat prevention. Enterprise Architecture is not only a proactive risk management tool, but it also contributes significantly to the overall business strategy. The integration of cybersecurity and enterprise architecture entails not only fortifying the technological infrastructure but also integrating it into the overarching business strategy. This enables the correlation of cybersecurity endeavors with the objectives of the organization, thereby connecting technological aspirations with business strategy. This study emphasizes the potential of incorporating adaptive and agile responses to threats into corporate culture to foster innovation. By functioning as a strategic catalyst, it assists organizations in adjusting to cyber threats, safeguarding business interests, and optimizing operations within an ever-evolving digital environment. By integrating governance and enterprise architecture frameworks, organizations can proactively mitigate business risks and cybersecurity threats, thereby fostering resilience and sustainability in the dynamic digital environment.

Keywords: Corporate Culture; Cybersecurity; Enterprise Architecture; Global Business; Risk Management.

1. Introduction

Today's digital era presents a unique challenge for businesses across industries due to technological advances and a widespread cyber threat landscape. The rise of complex, multi-layered cyber threats has forced organizations to rethink their strategies. Enterprise Architecture has become a foundation for building corporate Information Systems to strengthen defense and manage business risks in response to this urgent concern. Traditional defense mechanisms are vulnerable to more frequent, and complex cyberattacks. Data breaches, ransomware attacks, and system compromises disrupt operations and damage stakeholder trust. In the face of rapidly changing threats, detached and reactive cyber security

approaches need to be improved. To combat these evolving threats, businesses need a more holistic and proactive system that integrates technology, processes, and human factors.

Enterprise Architecture [1] is consistently recognized as a critical component in cyber security. Enterprise Architecture [2][3], organizes business goals and IT strategy to help organizations understand their technology landscape. EA helps organizations identify vulnerabilities and strengthen defenses by illustrating component relationships and dependencies. EA's full potential in addressing cyber security threats and business risks needs further exploration. This research aims to show how Enterprise Architecture methods can mitigate cyber security threats and manage business risks in response to the problems faced. This study examines the strategic integration of EA principles in organizations to identify benefits and drawbacks. The next step is to identify critical factors that can help Enterprise Architecture [4] be used as a proactive cyber defense while meeting business goals.

As the frequency and complexity of cyber security threats continue to rise, conventional defense mechanisms have been rendered vulnerable. System compromises, ransomware attacks, and data breaches not only disrupt operations but also erode stakeholder confidence. Traditional methods of cybersecurity, characterized by their fragmented and reactive nature, have demonstrated their insufficiency when confronted with swiftly evolving threats. Enterprises require a proactive and comprehensive approach that harmonizes human factors, processes, and technology to safeguard against these perpetually changing threats. Malicious software attacks, information leaks, and data theft are examples of cyber threats that have significantly disrupted business operations [5][6]. In addition, because of these incidents, the confidence of numerous related parties, including clients, business partners, and other stakeholders, has been eroded. Strategies that primarily concentrate on safeguards within the information technology infrastructure and responses to emerging risks have proven to need to be improved in addressing the proliferation of ever more complex threats.

Consequently, an all-encompassing and proactive strategy is required. Organizations require a strategic approach that encompasses effective technology utilization, rigorous process control, and a profound comprehension of human factors. Effective integration among these three components is critical when confronting ever evolving and progressively intricate threats. By adopting this comprehensive strategy, organizations can enhance their ability to withstand continuously evolving cyber risks, preserve uninterrupted operations, and preserve the confidence of their stakeholders.

Enterprise Architecture's [7] role in cyber security is becoming more evident to companies. EA uses a structured approach to align business goals with IT strategies, helping organizations understand their technology landscape. EA helps organizations identify vulnerabilities and strengthen defenses by defining component relationships and dependencies. Still, EA's full potential in addressing cyber security threats and business risks needs to be explored.

The objective of this study is to investigate and clarify the effectiveness of Enterprise Architecture in addressing cybersecurity threats while simultaneously managing the associated business risks. This study aims to examine the tangible advantages and disadvantages of strategically incorporating enterprise architecture principles within organizations. Moreover, the objective is to ascertain the crucial factors that contribute to the effective utilization of Enterprise Architecture as a proactive approach to mitigating cyber threats while simultaneously aligning with the broader business goals.

The primary objective of this study is to examine the efficacy of Enterprise Architecture in enhancing an organization's cybersecurity capabilities while concurrently mitigating the corresponding business risks. Moreover, the present study aims to investigate the primary obstacles encountered in the deployment of EAs that are specifically tailored to mitigate cybersecurity risks. The objective of this study is to analyze the challenges and intricacies faced by organizations during the integration of enterprise architecture into their cybersecurity framework. Additionally, it seeks to identify and describe the obstacles that impede the seamless implementation of EA. The research questions are as follows:

What are the optimal methodologies and essential determinants in the integration of enterprise architecture for comprehensive management of cyber security? (RQ 1). What is the impact of aligning enterprise architecture with business objectives on the enhancement of resilience against emerging cyber threats? (RQ 2).

This research seeks to contribute to knowledge and thinking regarding the application of Blueprint or Enterprise Architecture development as a strategic approach to facing the ever-evolving cyber threat landscape. The novelty lies in its comprehensive exploration of the integration of EA, not merely as a technological fortification but as an enabler of resilient business strategies in the face of cyber risks. This section sets the stage for an in-depth exploration of the strategic utilization of Enterprise Architecture to confront cyber security threats and manage associated business risks, aiming to uncover insights that will shape resilient and adaptive organizational strategies.

2. Research Method

2.1. Research Methodology

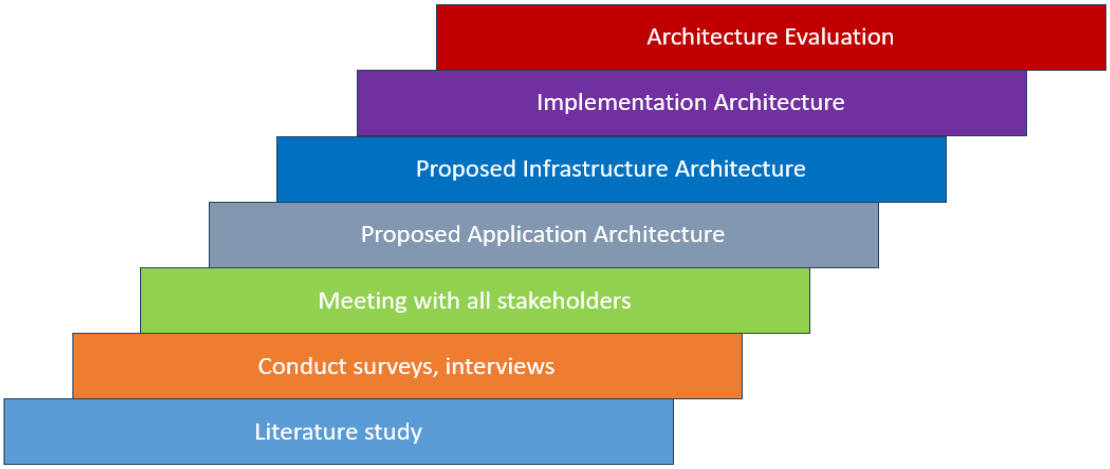

Figure 1. Methodology

Figure 1. Several critical procedures must be followed to establish a structured and effective system. The first step in comprehending the conceptual foundation and guiding principles of system development involves conducting an exhaustive review of the relevant literature. This stage provides the group with an in-depth understanding of successful best practices that have been tested in comparable environments. Through the utilization of surveys and interviews, a more comprehensive comprehension of the stakeholders was attained. By engaging in direct communication with them, it is possible to discern their needs, expectations, and obstacles, which subsequently serve as the foundation for developing suitable resolutions. Conduct meetings with all relevant parties to ensure that everyone agrees with the system development's shared objectives, scope, and requirements. Effective communication is crucial in this context as it guarantees that all parties have the same goal and align their expectations. Following this, the proposed Application Architecture will be designed. This stage entails the development of a comprehensive framework, the selection of appropriate technology, and the delineation of the application's overall structure. The Infrastructure Architecture and Implementation Architecture are subsequently meticulously designed. The presence of a robust infrastructure and efficient implementation are essential components for the seamless operation of applications. The architecture evaluation phase concludes with a review and verification that each element of the designed architecture satisfies the predetermined functional and non-functional requirements and is consistent with the system development's overarching objectives. Collectively, these phases constitute a crucial cornerstone in the construction of an organized, unified, and efficient system.

2.2. Cybersecurity

Cybersecurity serves as the principal barrier against a multitude of perilous entities that lurk in the digital domain. It comprises an intricate web of methodologies, installations, and controls that safeguard sensitive information, systems, and networks against malevolent entities. In the current era of globalization and device interoperability, where data flows effortlessly between nations and devices, cybersecurity cannot be overstated. It functions as an essential defensive mechanism, safeguarding governments, organizations, and individuals against an extensive array of cyber threats, including but not limited to sophisticated hacking endeavors, ransomware attacks, and phishing attempts. The principal objective is to fortify the availability, confidentiality, and integrity of systems and data, thereby guaranteeing their continuous operation amidst opposing forces.

The perpetual growth of cybersecurity reflects the ever-changing characteristics of the digital environment that it endeavors to safeguard. As a result of the increasing intricacy and sophistication of cyber threats, cybersecurity strategies must continuously adapt and develop. Achieving this requires an all-encompassing approach comprising proactive risk management, resilient security protocols, continuous monitoring, and swift incident response mechanisms. In addition to being a technological issue, cybersecurity is a field of study that incorporates human behavior, processes, policies, and technology. This necessitates a strong correlation between cutting-edge technologies, including artificial intelligence, intrusion detection systems, encryption, comprehensive policies, employee training, and a corporate environment that prioritizes cyber resilience. The significance of cybersecurity extends beyond individual entities and constitutes a critical component of both national security and global stability. Cyberattacks possess the capacity to cause widespread anarchy, compromise confidential government data, and disrupt critical infrastructure worldwide. Hence, governments, the private sector, and international institutions must work in concert to establish a resilient framework, exchange threat intelligence, and combat cyber threats collectively. Fundamentally, cybersecurity serves as an indispensable cornerstone of the digital

age, guaranteeing the safeguarding and dependability of the progressively interconnected systems that underpin our everyday existence, economies, and international engagements. Sustained development and adjustment are indispensable for preserving confidence, steadiness, and protection in the digital realm.

2.3. Intrusion Detection and Prevention System

Due to the expansion within the realm of cyber security, the Intrusion Detection and Prevention System (IDPS) is a critical component in safeguarding computer systems and networks. It is designed to identify, thwart, and respond to attacks that pose a risk of compromising the security of digital infrastructure or causing damage. Its primary function is to identify suspicious activity in the data traffic entering and exiting the network, provide alerts or take action to mitigate security risks and perform this function continuously. The IDPS functions as a foreman, observing network, system, and data activity in advance to predict potential attacks. This can include cyberattacks attempting to compromise a system or DDoS attacks that disrupt the availability of services by employing a range of detection techniques, including the utilization of established attack signatures, examination of atypical activity, and surveillance of network traffic patterns, IDPS endeavors to identify and address threats promptly.

IDS and IPS are the main IDPS types. IDS aims to identify suspicious activity or security breaches, enabling the provision of warnings to system administrators in preparation for subsequent actions. These two elements collaborate to establish a robust and adaptable barrier against ever-changing cyber threats. By examining network traffic and activity logs for atypical patterns that may signify an intrusion, this is achieved. In contrast, IPS possesses enhanced preventive capabilities in addition to detection capabilities akin to IDS. By interrupting the transmission of data identified as a threat or by automatically modifying access rules, an IPS can implement prompt measures to avert or obstruct identified attacks.

IDPS's primary function is to monitor network traffic and system activity in real-time. This requires the observation of data flow, transmitted, and received packets, and an assortment of additional network parameters. IDPS identifies attacks or suspicious behavior by employing methods and techniques, including behavior detection (behavior-based), anomaly detection (anomaly-based), and signature-based methods and techniques. Behavioral detection attempts to identify anomalous activity exhibited by users or systems, as opposed to signature methods, which compare known attack patterns with ongoing traffic. Anomaly detection, conversely, oversees routine traffic patterns and generates notifications if anomalous activity is identified. The implementation of an IDPS is crucial for safeguarding IT infrastructure against cyber threats. By utilizing a dual approach of detection and prevention, Intrusion Detection and Prevention Systems (IDPS) contribute to the preservation of system and network security, safeguarding against ever evolving and progressively sophisticated threats. Even with its pivotal function in safeguarding digital infrastructure, IDPS encounters several obstacles. This encompasses the issue of the propensity for false positives or false negatives, which may impede the precision of threat detection. Additionally, routine maintenance and complex configurations must be considered when attempting to optimize IDPS performance.

2.4. Enterprise Architecture

Enterprise Architecture, which is based on The Open Group Architecture Framework is a structured and holistic approach in developing organizational architecture. TOGAF provides comprehensive guidance in compiling, implementing, and managing architecture that includes business and technology aspects. This framework consists of several processes, methodologies, and tools designed to support planning and developing architecture that suits organizational needs. One key thing about TOGAF is its structured and iterative process cycle. This cycle is divided into several phases that include understanding business needs, architecture development, solution implementation, and continuous monitoring and updating. With this approach, organizations can understand their business needs more deeply, develop an architecture that supports strategic goals, and ensure effective implementation and continuously adapt the architecture to evolving needs.

TOGAF also offers flexibility in its implementation. This framework can be adapted to the specific needs of an organization without losing its integrity and basic structure. This allows organizations to adopt specific parts of TOGAF that are most relevant or appropriate to their situation without having to follow the entire framework, providing the ability to customize the architecture to suit the organization's internal and external conditions. One of the main advantages of TOGAF is its attention to balance between business and technology aspects. By considering business aspects such as strategy, processes, and customer needs along with the technology used, TOGAF enables organizations to design architectures that not only support current operations but also prepare the company for future growth and adaptation. Overall, TOGAF brings a structured and systematic concept to the development of Enterprise Architecture. Through its iterative, flexible approach and balanced attention to business and technology, TOGAF provides a powerful guide for organizations to design, manage and update architectures that are sustainable and meet evolving business needs.

The structured process cycle of TOGAF is regarded as a fundamental component. The framework encompasses four primary domains, specifically the delineation of architectural objectives, the progression of architectural design, the execution of architectural plans, and the oversight of architectural operations. The following framework offers a systematic approach to effectively oversee and direct the progression of a comprehensive architectural framework within an organizational context. The process commences with a thorough comprehension of business objectives and requirements, followed by the formulation of a suitable architectural framework. Subsequently, the planned solutions are

executed, and a continuous cycle of monitoring and updating is undertaken to ensure alignment with organizational and technological advancements. The TOGAF framework also provides a highly adaptable structure. This enables organizations to effectively modify and incorporate the architectural process with other pre-existing methodologies or approaches. The framework's modular design permits the utilization of select components without requiring the adoption of the entire structure. This feature offers the requisite flexibility to customize the architecture according to the specific requirements of an organization.

Furthermore, TOGAF places significant emphasis on both business and technology considerations. One of the notable benefits offered by TOGAF is its emphasis on achieving a harmonious equilibrium between business objectives and technological aspirations. This approach enables organizations to formulate architectures that not only fulfill present business requirements but also equip the organization for future expansion and adjustment to swift technological advancements. TOGAF facilitates the development of sustainable and scalable architectures for organizations by effectively addressing both business and technology considerations in a well-balanced manner. Finally, the TOGAF framework advocates for the implementation of optimal practices and the effective utilization of resources. TOGAF, as a framework, advocates for the adoption of industry-leading standards, established methodologies, and optimal practices for the purpose of designing and effectively managing architecture. This facilitates the optimization of resource utilization within organizations, mitigates the potential for ineffective implementation, and yields a resilient and adaptable architecture. In general, the utilization of the TOGAF Framework in Enterprise Architecture provides a comprehensive and well-organized structure for the management of organizational architecture. TOGAF is a precious instrument in the planning, development, and management of architectures that cater to the ever-changing requirements of business and technology. It achieves this through its emphasis on structured process cycles, flexibility, the establishment of a harmonious equilibrium between business and technology, and the careful selection of optimal practices.

3. Result and Discussion

3.1 Results

3.1.1. Application Architecture

This study uncovers the fact that a significant number of companies need to adequately safeguard their data by employing proactive strategies, such as security monitoring and the implementation of intrusion detection systems. The lack of preparedness for cyberattacks frequently results in companies operating reactively, needing more systems for proactive threat detection and prevention. Within this context, the current study provides organizations with proactive recommendations for bolstering their data security protocols to avert potential breaches. One of the primary recommendations involves the adoption of a heightened level of proactive security monitoring. This entails the utilization of tools and systems for the ongoing surveillance of network activity, the detection of anomalous patterns, and the prompt response to potential threats upon their identification. Furthermore, the integration of an intrusion detection system should be considered as a means for organizations to proactively identify and mitigate potential threats prior to any detrimental impact on their systems. By implementing a proactive strategy, organizations have the potential to reduce their susceptibility to cyber threats. In addition to expedited threat detection, there will be an accompanying opportunity to implement preventive measures prior to their substantial consequences. Hence, this study emphasizes the significance of implementing preventative measures to safeguard organizational data and effectively manage responsiveness in response to cyber threats.

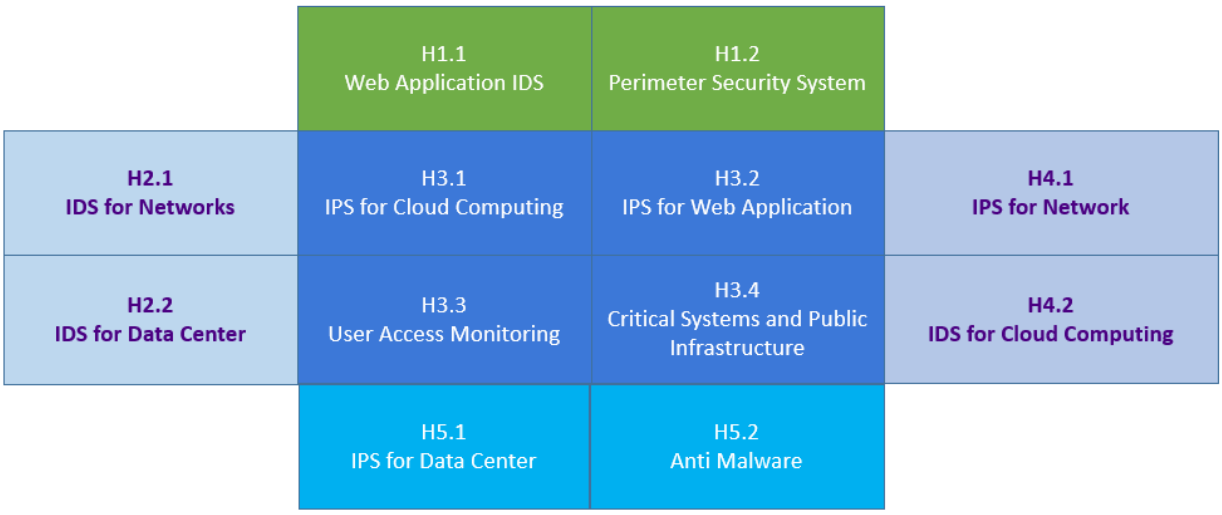

Figure 2. Application Architecture

Figure 2, the application architecture of Intrusion Detection Systems contributes significantly to protection against a wide range of cyber threats, especially in corporate networks, making it an essential component in ensuring security. Within a corporate network, an Intrusion Detection System (IDS) serves as a vigilant and diligent guardian, continuously monitoring the flow of network traffic, both from internal and external sources. The main goal of this system is to identify potential risks or questionable actions, such as phishing attacks and malware infiltrations. Through careful examination of the network flow, an Intrusion Detection System [8] functions as a proactive alert system, notifying administrators of any irregularities that may indicate malevolent motives or compromises in security. Furthermore, the incorporation of Intrusion Detection Systems (IDS) into the perimeter security framework, including firewalls and gateways, enhances the network's defensive capabilities. Situated strategically at these critical junctures, Intrusion Detection Systems (IDS) diligently monitor the flow of incoming and outgoing network traffic. From this perspective, Intrusion Detection Systems (IDS) can efficiently examine the data streams, promptly detecting potential external attacks or security breaches that specifically aim at compromising the network boundary of the organization. It functions as the primary line of defense, reinforcing the boundary to deter and repel potential intrusions from external entities. Moreover, the incorporation of Intrusion Detection Systems in data centers plays a crucial role in enhancing the security stance of essential server infrastructure. In the present context, Intrusion Detection Systems (IDS) undertake the responsibility of consistently monitoring and protecting servers and critical infrastructure components. The system carefully examines the flow of network traffic, promptly identifying and addressing possible risks such as Distributed Denial-of-Service (DDoS) attacks or penetration testing endeavors. The role of this entity is of utmost importance in guaranteeing the integrity and accessibility of critical data and systems.

The intrusion detection system plays a pivotal role in ensuring the security of data and applications that are hosted within cloud computing environments. The intrusion detection system can identify and addressing cyber threats that are unique to cloud services by examining the traffic that flows through the cloud infrastructure. This system plays a crucial role in protecting against potential risks that arise from the utilization of shared resources and virtualized environments. Furthermore, Intrusion Detection Systems play an essential role in the protection of vital systems and public infrastructure. This system is necessary for safeguarding and strengthening systems of critical infrastructure that are indispensable for the provision of public services. IDS is utilized across various sectors, such as energy, transportation, and healthcare. The system functions as a comprehensive surveillance mechanism, continuously monitoring and detecting potential threats that have the potential to disrupt critical services. Its primary objective is to maintain the uninterrupted operation of these services and protect the well-being of the public. In a wide range of applications, Intrusion Detection Systems function as a vigilant entity, adjusting its methodologies and detection techniques to suit different environments. The multifaceted nature of this technology renders it indispensable in various domains, such as monitoring user access, safeguarding web applications, ensuring the security of IoT devices, analyzing malware behaviors, and improving security testing methodologies. The significance of IDS in strengthening contemporary networks and systems against the ever-changing realm of cyber threats is emphasized by this comprehensive approach.

3.2. Infrastructure Architecture

Infrastructure architecture prepared with security objectives for companies is a crucial foundation in ensuring the protection and reliability of the systems and data they own. This architecture consists of a series of interrelated layers, which work together to protect enterprises from diverse and evolving cyber threats. First, the Server layer is the main center of this infrastructure. In it, the servers that run applications and store company data are located. Security at this layer is essential to protect access to sensitive information, and this is done through proper access settings, data encryption, and continuous monitoring for suspicious activity. The Network layer serves as the interconnecting backbone. Various systems and devices in a company network. Devices such as routers, switches, and other network infrastructure reside in this layer. Security at this layer is fundamental because it is the path for data to move between various devices. Data encryption, access control, and network traffic monitoring are vital in maintaining the security of this layer.

The Firewall and Intrusion Detection/Prevention System (IDS/IPS) [9][10], layers are at the forefront of a company's defense against external attacks. A firewall is responsible for inspecting and managing traffic in and out of a network, while an IDS/IPS actively monitors network activity to detect suspicious patterns or signs of threats. Both play an essential role in deterring attacks and providing rapid responses to identified threats. Finally, the Application Security layer is critical for protecting the applications used by the company. This includes security measures such as data encryption, strict access management, as well as implementing security practices in application development and maintenance. This layer is crucial because applications are often easy targets for cyber-attacks. By paying attention to these four layers, companies can build a solid and holistic security foundation. The combination of each layer provides comprehensive defense, ensuring that company systems and data are effectively protected from various cyber threats that can disrupt the company's performance and operational continuity.

Figure 3. Infrastructure Architecture

Figure 3 illustrates the Infrastructure Architecture, which serves as the fundamental basis for ensuring the security of an information system. This architectural design is structured into four distinct layers, providing a resilient framework for safeguarding, and overseeing an organization's digital resources. The initial layer, referred to as the Server layer, serves as the fundamental component of this infrastructure. Within the system, there exists a collection of servers that are responsible for delivering the necessary services and applications as demanded by the organization. This encompasses application servers, databases, and a range of other services. The significance of security at this layer cannot be overstated, as the server serves as the primary gateway for both internal and external users. Ensuring system stability and reliability necessitates prioritizing access management, physical security, and server health monitoring.

The subsequent stratum is the Network layer, serving as the fundamental infrastructure facilitating intercommunication among various systems. This layer encompasses network devices such as routers, switches, and other devices that govern the transmission of data within the network. Ensuring security at this layer is of utmost significance in safeguarding the integrity and confidentiality of data during its transmission across various points within the network. The implementation of data encryption, traffic monitoring, and appropriate network access configurations can effectively ensure this safeguard. The subsequent layer pertains to the Firewall/Intrusion Detection System (IDS) layer, which assumes the responsibility of safeguarding the perimeter security. A firewall functions as an initial line of defense that examines and regulates the flow of data traffic as it enters and exits a network. In the meantime, an Intrusion Detection System [11] is employed to actively monitor network activity with the aim of identifying and flagging any anomalous patterns or behaviors that could potentially indicate an attack or pose a threat to the system. The collaboration between the two entities serves the purpose of mitigating unauthorized access and effectively identifying and addressing potential cyber threats.

The Application Security layer serves as the primary safeguard against both internal and external threats that may compromise the integrity and security of the applications utilized within the organization. This layer encompasses a range of security technologies, including data encryption, user access management, and the implementation of security practices within application code to mitigate potential attacks such as SQL injection or cross-site scripting. Since malicious actors frequently target applications, it is of utmost importance to implement robust security measures at this level. By diligently focusing on these four layers, organizations can establish a powerful security framework within their infrastructure. The integration of these four layers enables IT managers to effectively deploy a holistic security approach, mitigate the likelihood of cyber threats, and ensure the protection of the confidentiality and integrity of the organization's data. And information systems.

3.3. Discussion

What are the optimal methodologies and essential determinants in the integration of enterprise architecture for comprehensive management of cyber security?

The integration of Enterprise Architecture for comprehensive management of cyber security entails a set of structured approaches that address complex challenges in the realm of digital security. An optimal methodology and crucial determinants guide these approaches. A risk-based approach is an effective methodology. In this scenario, the initial step in formulating a suitable security strategy is the process of identifying potential risks. Enterprise Architecture is a methodology employed to examine and delineate susceptible infrastructure, commercial procedures, and valuable resources, subsequently devising suitable security measures to alleviate such risks. An alternative approach involves the utilization of standards and compliance as a guiding framework. The integration of enterprise architecture in the field of cyber security pertains to the incorporation of globally acknowledged standards and frameworks, such as ISO/IEC 27001, NIST Cybersecurity Framework, or COBIT. Enterprise architecture implementations that effectively address these

Standards play a pivotal role in ensuring that security systems are following regulatory requirements and possess the capability to withstand a diverse array of cyber threats.

The establishment of an integrated security architecture is of utmost importance. This entails the development of a comprehensive system design, encompassing both the infrastructure level and the specific applications. The field of Enterprise Architecture holds significant importance in the context of organizational operations. Comprehensive analysis and incorporation of security measures across all levels of the architectural framework. This encompasses the identification of vulnerabilities and the subsequent identification and implementation of suitable strategies to fortify the existing defense mechanisms. In addition to this, the involvement of stakeholders, the factor mentioned above plays a pivotal role in ascertaining the result. The inclusion of multiple departments or business units in enterprise architecture planning and implementation is imperative. Effective communication among security teams, developers, business managers, and other stakeholders is crucial for successfully integrating enterprise architecture (EA) into comprehensive cybersecurity management. Continuous monitoring and evaluation are an essential component as well. After the implementation of an Enterprise Architecture, it is crucial to consistently monitor and evaluate its efficacy in mitigating emerging cyber threats. The dynamic nature of technology advancements and the prevalence of cyber threats necessitate the regular updating and adaptation of enterprise architecture to address emerging needs. By employing appropriate methodologies, such as a risk-based and standards approach, and giving due consideration to the integration of security architecture, involvement of stakeholders, and regular evaluation, the integration of Enterprise Architecture can serve as a robust basis for comprehensive and adaptable management of cyber security, aligning with the constantly evolving dynamics of cyber threats. To elaborate and expand upon the given topic.

What is the impact of aligning enterprise architecture with business objectives on the enhancement of resilience against emerging cyber threats?

The alignment of Enterprise Architecture with business objectives has been found to have a substantial influence on enhancing resilience to emerging cyber threats. When Electronic Arts is strategically aligned with the business objectives of organizations, it empowers them to adopt a comprehensive and proactive approach to addressing the constantly changing landscape of cyber threats. One of the effects is an enhanced comprehension of the risks associated with every business endeavor undertaken. Enterprise Architecture plays a crucial role in identifying vulnerabilities within infrastructure and business processes that may be susceptible to attacks. This, in turn, facilitates the formulation of comprehensive and focused security strategies.

Furthermore, the alignment between enterprise architecture and business objectives facilitates the implementation of well-informed decision-making processes in the management of technology investments. Enterprise Architecture plays a crucial role in comprehending the way a specific technology facilitates the achievement of business objectives. This understanding empowers organizations to make more informed and strategic choices regarding investments. This approach enables the optimization of resource utilization and enhances managerial efficacy, emphasizing the seamless integration of security considerations into the initial stages of technology development or implementation.

When Electronic Arts is aligned with well-defined business objectives, it facilitates expedited decision-making processes and effectively adapts to emerging threats. In the context of a dynamic and evolving business landscape, the synchronization of organizational goals and security strategies enables enhanced adaptability and agility. The implementation of an integrated enterprise architecture facilitates the development of a robust infrastructure capable of promptly adjusting to dynamic circumstances, thereby enhancing the speed and efficacy of addressing emerging cyber threats. Furthermore, the alignment between enterprise architecture (EA) and business goals serves to improve the overall awareness of cyber security within the organization. This initiative aims to enhance the company's organizational culture by fostering a proactive approach to addressing cyber threats. It seeks to elevate awareness and instill a heightened sense of concern among all members of the organization regarding the adoption of robust security practices. This contributes to enhancing the organization's comprehensive defensive strategy, as each member within the company actively participates in the endeavor to uphold security measures.

In general, the alignment of enterprise architecture with business objectives serves as a robust basis for enhancing organizational resilience in the face of dynamic cyber threats. Through the facilitation of enhanced risk comprehension, more strategic allocation of technology investments, expedited response to emerging threats, and the cultivation of fortified security culture, this integration assists organizations in constructing resilient frameworks to effectively navigate the dynamic security landscape of the contemporary digital era.

3.4. Limitation

This study exposes the shortcomings of its proposal, which centers on the implementation of infrastructure and applications for cyber security. Further investigation is warranted to delve into more intricate and all-encompassing implementations, with a particular emphasis on security applications and infrastructure within enterprise information technology networks.

3.5. Feature Work

It would be critical to delve deeper into the discussion of implementation. This may encompass comprehensive methodologies for integrating cyber security applications into the IT infrastructure of an organization, including intrusion detection systems, data encryption, and identity management. Furthermore, an emphasis on infrastructure necessitates a more comprehensive examination encompassing design, configuration, and network management, which must effectively integrate security layers. Further research in this area might investigate case studies that encompass practical implementation across a range of business scenarios. This enables one to comprehend the potential obstacles that may emerge throughout the implementation phase, in addition to devising efficacious resolutions to address these issues. Additionally crucial is the delineation of risk management facets pertaining to the implementation of security measures. By prioritizing risk assessment, security policy formulation, and post-implementation performance evaluation of security systems, a more comprehensive comprehension of the efficacy of the measures undertaken can be attained. Further investigation into these domains may yield a more holistic and applicable understanding of how infrastructure implementation and cyber security can be executed more effectively in enterprise information technology network environments.

4. Related Work

An examination of the significance of Enterprise Architecture in reducing business risks and cyber threats reveals an expanding corpus of scholarly literature that underscores its critical influence. The significance of this as a proactive barrier against ever-changing cyber threats, in line with the strategic objectives of businesses, has been emphasized in numerous studies. The inquiry scrutinizes the approaches utilized by EA to fortify cyber resilience, and its incorporation with risk management strategies is implemented to ensure protection against potential risks and an extensive array of threats. The subsequent investigation pertains to the subsequent investigation: Cyber-threat intelligence (CTI) is increasingly important in supporting enterprises, but its adoption rate is low. The literature on CTI is heavily dominated by technology, leaving gaps in knowledge. This study explores theoretical foundations, practice research methods, and the role of artifacts, objects, and information systems in CTI implementation [12]. This article introduces a methodology that is tailored to smart grids, which integrates risk assessment and threat modeling. The objective is to develop a comprehensive set of security requirements for the integration of renewable energy into a low-voltage grid architecture [13]. This research paper proposes a threat modeling framework for intelligent cyber-physical systems (CPS) to identify potential security risks. It uses the MITRE ATT&CK matrix and system requirement collection to generate a threat list for an intelligent firefighting system, demonstrating its potential for protection and mitigation [14]. This study examines the security risks and challenges of Ag-IoT technology, focusing on emerging applications, architectures, suspected cyber-attacks, and challenges in incident response and digital forensics. It concludes that ensuring security is crucial for uninterrupted services and effective investigation in the smart agricultural sector [15]. Cyber-attacks impact our lives, requiring cooperation for cyber-security and safety. A five-level trust model for cloud-edge data-sharing infrastructure addresses concerns about the confidential sharing of CTI. The model allows data owners to choose trust levels and sanitization approaches, with implementation and testing conducted by four pilot projects [9]. CAESAR8, a novel approach, advocates for the implementation of dynamic and holistic evaluations pertaining to information security risks within IT projects. It assesses the maturity of security considerations in eight domains, addressing real-world problems, especially for smaller organizations [16].

5. Conclusion

The digital era presents a unique challenge for businesses due to technological advances and a widespread cyber threat landscape. Enterprise Architecture has become a foundation for building corporate Information Systems to strengthen defense and manage business risks. Traditional defense mechanisms are vulnerable to more frequent, and complex cyberattacks, such as data breaches, ransomware attacks, and system compromises. This study investigates the effectiveness of Enterprise Architecture in addressing cybersecurity threats and managing associated business risks. Intrusion Detection Prevention System is a crucial component in cybersecurity, designed to identify, thwart, and respond to cyber threats. The Open Group Architecture Framework is a structured approach to developing organizational architecture that includes business and technology aspects. Intrusion Detection Prevention System are essential in protecting against various cyber threats, particularly in corporate networks. The Infrastructure Architecture, structured into four layers, provides a resilient framework for safeguarding an organization's digital resources. Several actionable suggestions for organizations to implement:

1) It is imperative for organizations to perform routine security assessments. This entails conducting regular security audits to detect any weaknesses or gaps in their systems. By completing routine monitoring and evaluation, organizations can expedite the implementation of preventative or corrective measures.

2) Software and Operating System Updates: Ensuring the regular updating of software and operating systems employed by the organization is of utmost importance. Frequently, these updates encompass security patches that serve to fortify the system against recently emerged threats.
3) Training of Personnel on Information Security It is critical to provide employees with ongoing training on information security practices. Personnel must be cognizant of potential dangers and possess the ability to identify and report suspicious circumstances.
4) The implementation of an IDS (intrusion detection system): The establishment of a sophisticated and efficient IDS system will empower organizations to promptly identify and address suspicious activities, thereby averting system compromise.
5) Development of an Incident Response Plan: The organization must establish a comprehensive incident response plan. It addresses procedures to be followed in the case of a cyberattack or security breach, including data and system recovery.
6) Monitoring and Analysis of Security Trends: Monitoring and analyzing security trends can aid in the prediction of future threats. This enables institutions to mitigate the risks associated with expected threats proactively.

References

[1] Hindarto, D., Indrajit, R.E. and Dazki, E., 2021. Sustainability of Implementing Enterprise Architecture in the Solar Power Generation Manufacturing Industry. *Sinkron: jurnal dan penelitian teknik informatika*, *6*(1), pp.13-24. DOI: https://doi.org/10.33395/sinkron.v6i1.11115.

[2] Amanda, D., Hindarto, D., Indrajit, E. and Dazki, E., 2023. Proposed use of TOGAF-Based Enterprise Architecture in Drinking Water Companies. *Sinkron: jurnal dan penelitian teknik informatika*, *8*(3), pp.1265-1277. DOI: https://doi.org/10.33395/sinkron.v8i3.12477.

[3] Iswahyudi, I., Hindarto, D. and Indrajit, R.E., 2023. Digital Transformation in University: Enterprise Architecture and Blockchain Technology. *Sinkron: jurnal dan penelitian teknik informatika*, *8*(4), pp.2501-2512. DOI: https://doi.org/10.33395/sinkron.v8i4.12977.

[4] Hindarto, D., 2023. Blockchain-Based Academic Identity and Transcript Management in University Enterprise Architecture. *Sinkron: jurnal dan penelitian teknik informatika*, *8*(4), pp.2547-2559. DOI: https://doi.org/10.33395/sinkron.v8i4.12978.

[5] Hindarto, D. and Santoso, H., 2021. Android APK Identification using Non Neural Network and Neural Network Classifier. *Journal of Computer Science and Informatics Engineering (J-Cosine)*, *5*(2), pp.149-157. DOI: https://doi.org/10.29303/jcosine.v5i2.420.

[6] Hindarto, D. and Santoso, H., 2022. Performance Comparison of Supervised Learning Using Non-Neural Network and Neural Network. *Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI*, *11*(1), pp.49-62. DOI: https://doi.org/10.23887/janapati.v11i1.40768.

[7] Sari, R.T.K. and Hindarto, D., 2023. Implementation of Cyber-Security Enterprise Architecture Food Industry in Society 5.0 Era. *Sinkron: jurnal dan penelitian teknik informatika*, *8*(2), pp.1074-1084. DOI: https://doi.org/10.33395/sinkron.v8i2.12377.

[8] Hasan, M.K., Habib, A.A., Shukur, Z., Ibrahim, F., Islam, S. and Razzaque, M.A., 2023. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications*, *209*, p.103540. DOI: https://doi.org/10.1016/j.jnca.2022.103540.

[9] Chadwick, D.W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A. and Wang, X.S., 2020. A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future generation computer systems*, *102*, pp.710-722. DOI: https://doi.org/10.1016/j.future.2019.06.026.

[10] Mantha, B., de Soto, B.G. and Karri, R., 2021. Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. *Sustainable Cities and Society*, *66*, p.102682. DOI: https://doi.org/10.1016/j.scs.2020.102682.

[11] Varga, S., Brynielsson, J. and Franke, U., 2021. Cyber-threat perception and risk management in the Swedish financial sector. *Computers & security*, *105*, p.102239. DOI: https://doi.org/10.1016/j.cose.2021.102239.

[12] Ainslie, S., Thompson, D., Maynard, S. and Ahmad, A., 2023. Cyber-Threat Intelligence for Security Decision-Making: A Review and Research Agenda for Practice. *Computers & Security*, p.103352. DOI: https://doi.org/10.1016/j.cose.2023.103352.

[13] Marksteiner, S., Vallant, H. and Nahrgang, K., 2019. Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling. *Journal of Information Security and Applications*, *49*, p.102389. DOI: https://doi.org/10.1016/j.jisa.2019.102389.

[14] Zahid, S., Mazhar, M.S., Abbas, S.G., Hanif, Z., Hina, S. and Shah, G.A., 2023. Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls. *Internet of Things*, *22*, p.100766. DOI: https://doi.org/10.1016/j.iot.2023.100766.

[15] Rudrakar, S. and Rughani, P., 2023. IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics. *Information Processing in Agriculture*. DOI: https://doi.org/10.1016/j.inpa.2023.09.002.

[16] Loft, P., He, Y., Yevseyeva, I. and Wagner, I., 2022. CAESAR8: An agile enterprise architecture approach to managing information security risks. *Computers & Security*, *122*, p.102877. DOI: https://doi.org/10.1016/j.cose.2022.102877.

