The Eastasouth Journal of Information System and Computer Science
Vol. 3, No. 02, December 2025, pp. 271-291
ISSN: 3025-566X, DOI: 10.58812/esiscs.v3i02

Cybersecurity in ERP-Integrated Supply Chains: Risks and Mitigation Strategies

Ravindra Khokrale
Sr. Solution Architect, Circular Edge LLC, USA

Article Info

Article history:

Received Dec, 2025
Revised Dec, 2025
Accepted Dec, 2025

Keywords:

Cyber Risk Management;
Data Integrity;
ERP Security;
Secure Integrations;
Supply Chain Cybersecurity;
Third-Party Risk

ABSTRACT

Cybersecurity risks have emerged as a burning issue as global supply chains increasingly use Enterprise Resource Planning (ERP) systems to integrate official systems into their supply chains. ERP systems unite different stakeholders, including suppliers, logistics, and finance teams, making it possible to exchange real-time information and streamline it. However, there is a possibility of cyberattacks in these systems, particularly when integrating with third-party systems, having poor access control, and using outdated software. The emergence of high-profile attacks such as the 2017 NotPetya has underscored the dramatic financial and operational loss factors because of ERP breaches and outlined the importance of firm protection against cyberattacks. This paper discusses the most significant cybersecurity threats to ERP-integrated supply chains and voices the successful mitigation measures. Major risks observed are the vulnerability of third parties, weak access control, and the use of old ERP systems. Such measures as multi-factor authentication, continuous monitoring, and vendor risk management are also evaluated as the best practices of the study. The study provides effective suggestions that can be implemented in organizations to ensure that their ERP-based supply chains are secured, and the chances of data breaches and disruptions in operations are reduced. With the digitalization of supply chains, the future is seen to utilize the new capabilities to use new technologies, including artificial intelligence and blockchain, to further improve the security and information integrity of ERP.

Corresponding Author:

Name: Ravindra Khokrale
Institution: Sr. Solution Architect, Circular Edge LLC, USA
Email: ravindravid@gmail.com

1. INTRODUCTION

The modern supply chains have been recognized to be supported by Enterprise Resource Planning (ERP) systems, including SAP, Oracle, and Microsoft Dynamics, which have made it possible to incorporate different business operations that include procurement, logistics, inventory control, and finance. Such systems allow the real-time exchange of information between the suppliers, manufacturers, and logistics companies and can facilitate efficient operation, the simplification of communication, and better decision-making. For example, the ERP solutions of SAP have linked more than 400,000 enterprises in the world, where organizations are able to maintain their supply chains in a more visible and controlled manner. With these different

functions integrated into one, these functions can be automated to save costs of operation and ultimately improve productivity. ERP also allows businesses to track and dynamically modify the activities of the supply chain and helps to maintain better coordination, delivery of orders on time, as well as an optimal use of inventory.

The role of ERP systems in the supply chains cannot be undervalued because they enable the availability of important information in real time, which helps in improving decision-making. In a new study by the International Data Corporation (IDC), 7 out of 10 companies state that there was a healthy rise in efficiency and decision-making in the firms since the adoption of ERP systems [1;2]. For example, logistics personnel will be able to immediately monitor the state of shipment, inventory, and order deliveries, and financial personnel will have access to the latest costs and revenues data, which will assist in financial planning and analysis. ERP systems also help companies to react more quickly to changes in the market and to the disturbances in the supply chain, which serves as a source of competitive edge and market resilience.

Although ERP systems have proven to be useful when they are integrated into supply chains, they bring major cybersecurity threats, and this is mostly because of the interdependency among modern supply networks. The increased use of third-party suppliers and cloud-based solution platforms in the supply chain activities provides weak points that are likely to be used by cybercriminals to operate. Since most ERP systems are used to store sensitive business information, including inventory level, financial transactions, and production plans, a breach could lead to dire consequences, including loss of money, theft of information as well and interference in business operations.

These risks have been brought into the limelight by high-profile cyberattacks. A notable incident is the 2017 cyberattack at NotPetya that targeted the major and significant global supply chains, such as Maersk and Merck [3]. This attack disrupted the operations of the shipping and port operations of Maersk, leading to losses of an estimated 300 million dollars because it crippled the operations of the company. Merck also had major operational losses, where the attack corrupted important data and impacted its production schedules. These incidences highlight how vulnerable the supply chains that are integrated into the ERP system are to cyber threats, hence the importance of having a solid security provision.

This paper will examine potential cybersecurity threats within ERP-integrated supply chains and discuss the possible mitigation strategies. The objectives of this study are:

1. To determine major cyber risks related to ERP systems in a supply chain, such as third-party risks, vulnerability to weak access controls, and the use of outdated software.
2. To investigate current cybersecurity strategies and the best practices used by organizations to protect their ERP systems.
3. To offer practical, real-world advice that several businesses can undertake to counter ERP-related cybersecurity threats and protect their supply chains.

The area of this research involves investigating the issue of cybersecurity in structurally ERP-integrated supply chain management in several sectors, including manufacturing, logistics, and retail. The investigation will deal with external and internal sources of risk, such as third-party vendors, poor user access control, and old ERP systems. The research will also present a global view of how organizations in various parts of the world (e.g., North America, Europe, and Asia) are dealing with these issues using case studies and industry examples.

To fulfill its objectives, this research is structured in various chapters. The Literature Review chapter discusses the current research on ERP security risks and mitigation

measures. The methods chapter indicates the methods of data collection and analysis. The Results chapter shares the outcomes of the study, and the Discussion chapter is the evaluation of the effectiveness of different mitigation strategies. In the Future Research Recommendations section, the avenues to be researched further are noted, and the Conclusion chapter entails a recap of the most significant findings and practical advice on securing ERP-integrated supply chains. Every chapter expands on the others to provide an all-encompassing conclusion towards the security of ERP within the present-day supply chains.

2. LITERATURE REVIEW

2.1 *Overview of ERP-Integrated Supply Chains*

Enterprise Resource Planning (ERP) systems have become business necessities to supply chains in contemporary society since a wide range of processes can be integrated through ERP systems to include procurement, logistics, inventory management, and financial tracking. These systems are aimed at simplifying the processes through the unifying central platform in which real-time information is circulated through the departments. The ERP systems allow smooth integration among the partners of the supply chain, as it leads to quick decision-making and operational efficiency [4]. For example, SAP and Oracle are common ERP solutions that combine systems order management, supplier relations, and production scheduling, and therefore improve real-time information circulation across global supplying chains.

The supply chain management of the global adoption of ERP systems is significant. Statista also states that in 2020, 46% of companies in the world used ERP to coordinate their supply chain activities. The extensive use of ERP systems indicates that they provide the necessary effect on enhancing the level of operational transparency and promoting efficiency in the supply chain control [5]. Such systems enable businesses to respond more effectively to shifts in demand, supply, and production timetables, resulting in a reduction of operational costs and effective resource redistribution. ERP systems integration with cloud technologies has offered companies more flexibility, as the company can scale its operations and also have access to real-time data in various locations.

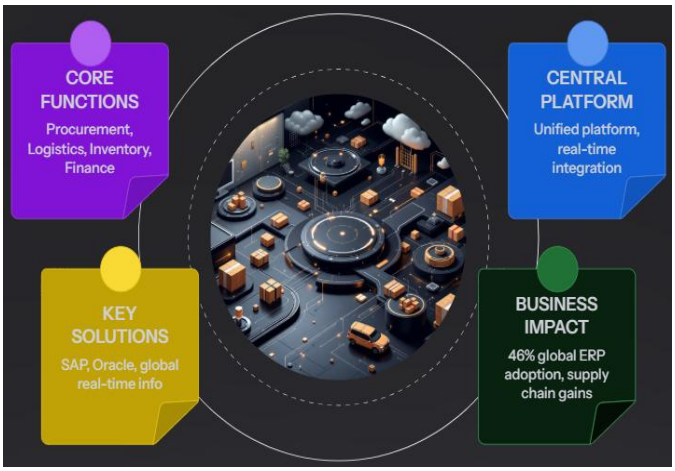

Figure 1. The adoption of ERP systems in supply chains by focusing on core processes, real-time information sharing, and international adoption of ERP in improving operational efficiency.

2.2 *Overview of ERP-Integrated Supply Chains*

Figure 1 illustrates the consolidation of central operations in contemporary ERP systems, which include procurement, logistics, inventory management, and finance. These systems are centralizing and unifying data to

enable real-time communication amongst supply chain partners, which improves operational efficiency and decision-making. SAP and Oracle are major solutions that have been widely used to facilitate order management, supplier relations, and production scheduling to enhance better operations of the global supply chain. Another important point that the image makes is the high rates of international applications of ERP systems, with 46% of the firms using these systems to manage their supply chains. The connectivity of ERP systems to cloud technologies also contributes to the increase in flexibility, providing businesses with the ability to expand and increase real-time information, resulting in improved resource utilization and lower operation expenses.

2.3 *Cybersecurity Risks in ERP-Integrated Supply Chains*

Although the advantages of ERP systems can be hard to overlook, cybersecurity threats are also present since the supply chains are becoming more intertwined and depend on third-party providers. Incorporating the external partners into the ERP systems introduces vulnerabilities that may be exploited by the cybercriminals. Among the risks is the vulnerability of the third-party, where the supply chain faces failure if its security practices by the suppliers' or vendors turn out to be a weak point. For example, the 2013 Target breach was associated with a third-party vendor that had insufficient secured systems, and sensitive customer information was exposed [6]. This incident shows that poor security in third-party integrations could lead organizations to cyberattacks.

Another major vulnerability of ERP systems is weak access controls. A poor authentication system is a common cause of data breaches, where an unauthorized user can access sensitive information. According to a study conducted by Ponemon Institute, it was established that poor access control measures contributed to 63% of data breaches [7]. This may present in the form of employees or third-party contractors gaining needless access to the important components of the system in the ERP system, and may result in the editing or stealing of data.

Big data is also concerned with data integrity. Alteration or graft of data can interrupt the production schedule, inventory, and finances. Such networks as ERP systems can be quite vulnerable to such an attack because they depend on the quality of information in decision-making. Indicatively, manipulated inventory information may result in wrong stock levels, which will disrupt production and delivery of orders. Maintaining data integrity in ERP systems is thus an important tool that can ensure the functionality of supply chains.

Outdated ERP software also puts a company at risk of cybersecurity threats. According to Forrester (2020), 45% of firms have obsolete ERP systems that hackers can easily attack. Such systems do not have important security patches and are thus prone to attacks by cybercriminals [8]. Lack of updating ERP systems with new security features and patches may have adverse taxing impacts, including hacking or even ransomware attacks. ERP is dynamic, and the up-to-date software is a vital aspect in addressing the possible cybersecurity threats.

2.4 *Importance of Cybersecurity in the Digital Supply Chain*

Due to the increasingly digital nature of supply chains, the cybersecurity risks linked to supply chains have increased by a significant margin. Accenture surveyed in 2020, revealing that 71% of companies had an incident of a cybersecurity breach that started with a third-party supply chain partner [9]. The increasing significance of tackling the cybersecurity risk in the digital supply chain is highlighted by this statistic. As digital tools, such as ERP systems, are becoming more and more part and parcel

of all supply chain processes, even a single shift in cybersecurity can be felt in long-lasting effects, not just in the form of financial damages but also loss of prestige and confidence among customers. Research on the outcomes of a breach in a digital supply chain is serious. Data breaches can have a high financial cost; in 2020, IBM reported the average price of a data breach to be $3.86 million. Such violations may involve direct financial damage, especially in businesses with sensitive information like manufacturing, retailing, and pharmaceuticals [10].

The breaches usually result in production delays that may further worsen the economic losses and influence the business continuity. For example, breach of data may stop production lines, because shipment delays, as well as inventory interruption, which negatively affect the capacity of a company to satisfy its customer needs. The lack of breach in the ERP-integrated supply chains may destroy the trust of the customers. Firms that neglect to secure sensitive information also risk losing their reputation in the market, which might affect the long-term outcome of customer loyalty and brand value. In the globalized world where consumers demand secure and punctual delivery, supply chain breaches not only incur financial losses but also create a long-term tarnish to the image of the company.

2.5 *Existing Mitigation Strategies*

Several mitigation measures have been put in place by organizations to achieve ERP-integrated supply chains. The introduction of secure access controls is one of the key steps that can be taken. Two strategies that can be used to restrict entry to important system components are multi-factor authentication (MFA) and role-based access control (RBAC). Organizations should consider using several methods of identification or using user roles as a way of limiting access to sensitive ERP data to minimize potential cases of unauthorized access to the data [11]. Such measures are the most efficient in averting insider threats and reducing the possible harm resulting from compromised accounts.

Patching and updating should also be undertaken on a regular basis to ensure the ERP systems are secure. ERP vendors routinely issue security patches to mitigate vulnerabilities that are also occasionally found. Through updating systems on a regular basis, companies can minimize the chances of a cyberattack that exploits a known vulnerability in their software. For example, organizations such as Coca-Cola have also put in place round-the-clock monitoring and routine patching timelines to make sure that their ERP systems remain not vulnerable to external threats [12].

Another important measure of securing ERP-integrated supply chains is vendor risk management. Firms should evaluate the cybersecurity behavior of their third-party suppliers and partners to verify that they meet the required standards of security. A business can reduce the risks that are experienced as a result of third-party relationships by embedding cybersecurity requirements into contracts with vendors and completing periodic evaluations. The examples of businesses such as Coca-Cola have shown how checking vendors and engaging in constant analysis have been used to enhance the security of supply chains by revealing weak areas before they are exploited [13]. Digital supply chains cannot be secured with ERP systems without a multi-faceted strategy, which might encompass strong access control, frequent updates, and vendor risk management. Through these measures, organizations will be in a position to minimize their vulnerability to cybersecurity threats and improve the overall strength of their supply chains.

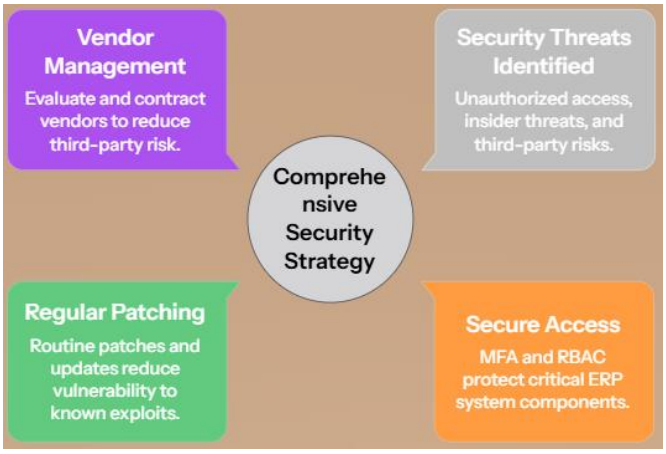

Figure 2. Key control mechanisms of securing ERP-integrated supply chains; secure access controls, frequent patching, maintenance of vendor management, and threat identification.

Figure 2 depicts the significant aspects of an ERP security strategy. It highlights the significance of vendor management to minimize third-party risks, the fact that security threats, including unauthorized access and insider threats, should be identified, and safe access based on multi-factor authentication (MFA) and role-based access control (RBAC) is required to protect sensitive system elements. Another important issue illustrated in the image is the importance of regular patching, whereby routine updates and security patches can help guard against the known vulnerabilities of ERP systems. These are a part of a multi-level strategy to implement the security of ERP-mediated supply chains since companies, such as Coca-Cola, have round-the-clock monitoring and vendor procedures to reduce risks and provide general security in the supply chains. This combination method assists in avoiding cyberattacks and minimizing the consequences of possible breaches.

3. METHODS AND TECHNIQUES

3.1 Data Collection Methods

The research involved both quantitative and qualitative research methods to obtain detailed data on both cybersecurity risks of the ERP-integrated supply chains and the effectiveness of mitigation strategies.

a. **Quantitative Approach:** The survey was done based on supply chain professionals and cybersecurity managers to get quantitative data. The purpose of the study was to evaluate the security practices of ERP and determine the vulnerabilities that were prevalent in ERP systems. The sample used for the survey was 200 practitioners in logistics and manufacturing industries, and the survey targeted the security levels in their respective organizations, the number of security breaches, and the extent to which the breaches affect the supply chain operations. Such a method enabled gathering some statistical data about the prevalence of ERP vulnerabilities, the actions undertaken to reduce risks, and the competence of the current security strategies. This approach was also used in the study of automated data validation in financial systems, and the role of measurement of security practices in industry-specific settings is significant.

b. **Qualitative Approach:** The analysis of in-depth case studies was also used to analyze actual events of organizations that encountered an ERP security breach. A case study that was one of them was based on what Maersk did in response to the 2017 NotPetya attack that interfered with their worldwide supply chain

operations [14]. This paper found the way Maersk detected vulnerabilities in their ERP system and responded to the incident, as well as what insights they learned about themselves regarding this major cyberattack. The same case study approach was used to examine the problems of power efficiency in hardware verification, demonstrating the efficacy of a comprehensive analysis conducted as part of a specific context and revealing underlying flaws in the system and ways to resolve them [15].

3.2 Data Analysis

The statistical software, SPSS, was also used to analyze the collected survey data in order to determine the trends and correlations regarding ERP security risks and mitigation measures. Statistical techniques helped to give some information about the rate of security breaches, the time of detecting and responding to breaches, and the effectiveness of various mitigation measures.

Key Metrics

In the analysis, a number of metrics were taken into consideration to determine the magnitude and the effect of a security breach in ERP systems. The percentage of companies that reported having a security breach as a result of ERP vulnerabilities was one of the metrics of interest. The survey data indicated that about 30 percent of companies affirmed that they had suffered breaches due to ERP security vulnerabilities. This percentage is an indication of how vulnerable the ERP systems are to cyber-attacks despite the sheer use of security tools. The other important indicator was the time taken to identify and act on breaches.

Analysis of data has indicated that 72% of all security breaches in ERP systems remained undetected for more than six months, and that is a high delay in detection and response time to breaches. The statistics were related to the outcomes of prior cybersecurity studies that also focused on the delay in the exploitation of weaknesses in sophisticated systems. Response breakdown based on industry, company size, and geographical location was made possible using SPSS, thereby making ERP security practices more granular. This also assisted in determining industry-specific problems and the comparative efficiency of various mitigation measures in the different sectors.

Table 1. ERP security breach key indicators including the percentage of companies that were targeted by the breach and the large gap between the breach and response times.

Metric	Value	Insight	Impact
Percentage of Companies with Security Breaches	30% of companies experienced breaches due to ERP vulnerabilities	Indicates vulnerability of ERP systems despite security measures	ERP systems are vulnerable to cyber-attacks
Time to Detect and Respond to Breaches	72% of breaches undetected for over 6 months	High delay in detection and response time	Delays in detection can worsen the impact of breaches

Table 1 provides the most important results of the data analysis of ERP security breaches. It focuses on two crucial measures, including the proportion of organizations that experience breaches and the response time to these breaches. This table demonstrates that 30% of firms experienced breaches involving ERP vulnerabilities, which highlights the vulnerability of the security despite its practice. It also indicates that 72% of breaches took more than half a year to be identified, meaning that there was a high ordeal in identifying and responding to breaches. These insights demonstrate a weakness of ERP systems and how the speed of detection affects the degree to which cyberattacks can be significant.

3.3 Risk Assessment Framework

The risk assessment framework was created to give a risk score to the various ERP security threats depending on their effects and the probability of danger. This model entailed considering all the external and internal risks associated with ERP systems and finding their comparative severity.

a. **Scoring Method:** The scoring system formed a scale between 1 and 5, with 1 being the lowest risk and 5 being the highest risk. The security risks were classified as four main risks, such as third-party vendor risks, lax access control policies, out-of-date software defects, and issues with data integrity. For example, third-party risks and data integrity received a greater score because they directly affected operational continuity and financial losses. Implementation risks, like poor access controls, though considerable, were considered less likely to lead to serious disruptions when appropriate access management systems were implemented.

b. **Financial Impact of breaches:** It was one of the important metrics in the structure of the risk assessment. The economic damages caused by the violations related to ERP could be quite significant in most cases, and companies report an average cost of $3.86 million per data breach in 2020 (IBM) [16]. Another critical metric, which was deemed essential, was the downtime within the system because the ERP was often infected by security breaches, resulting in a halt in operations. The reputational damage metric, which is more difficult to measure, also formed part of the assessment as breaches usually drive out customer confidence and adversely affect brand reputation. The cybersecurity researchers have applied similar frameworks to analyze the general risks that vulnerabilities of digital systems reflect [17].

3.4 Evaluation of Mitigation Strategies

Mitigation strategies applied by organizations in order to protect their ERP systems were tested according to the survey results and by analyzing the case study. A common set of methods that were considered was securing control access, upgrading software on a regular basis, and the practice of vendor risk control.

a. **Security Tools:** The paper aimed at testing the efficiency of particular security tools as ERP-specific firewalls, software to scan vulnerabilities, and identity management systems. A major decrease in breaches and unauthorized access was observed in companies that had adopted multi-factor authentication (MFA) and role-based access control (RBAC). This was especially so when it comes to organizations whose industries, such as manufacturing and logistics, are common targets of sensitive data, such as inventory levels and order information. Vulnerability scanning software was identified as useful to identify vulnerabilities in the ERP systems in time, eliminating the potential likelihood of attacks. These results are in tandem with the given practices, in which the focus on constant system verification assists in unauthorized permission prevention.

b. **Response Times:** The response time to vulnerabilities was also a crucial measure used to assess the efficacy of ERP security measures. Gartner (2020) revealed that the average company required 38 days to patch identified ERP vulnerabilities according to the survey results [18]. This lag in patching vulnerabilities was deemed a major problem since most attacks use known software weaknesses, which can be fixed with timely updates. Companies that had routines of patch management and

automated updates recorded much less response time and successful cyberattacks.

The mitigation strategies review showed that although other organizations have established effective actions, most of them continue to face delays in patching ERP security gaps and addressing third-party risks. The paper emphasizes the significance of proactive risk management and monitoring in order to ensure that the ERP-based supply chains are secure.

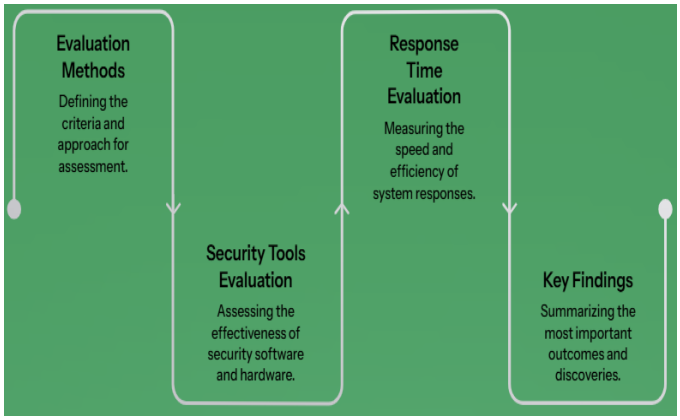

Figure 3. The key evaluation tools to evaluate the ERP security such as security tools evaluation, the evaluation of the response time, and the summary of the main results of the research.

Figure 3 shows the main aspects of ERP security protection methods, and it revolves primarily around the analysis of the security tools, how quick the teams are in responding to the issue, and the overall efficiency of the security measures. The flowchart also emphasizes Security Tools like multi-factor authentication (MFA), role-based access control (RBAC), and vulnerability scanning software, which were found to help lower unauthorized access and breaches. Response Time Evaluation is also significant, and the study discovered that an average company spent a period of 38 days to fix the vulnerability, which underscores the need to update themselves in time to avoid cyberattacks. The figure highlights the necessity of Proactive Risk Management to solve patching delays and third-party threats, constantly monitor them, and improve the security of the ERP-mediated supply chains.

3.5 Ethical Considerations

The ethical considerations throughout this study were important and relevant. In the research, informed consent was sought from all the survey participants and case study organizations, and there was a proper explanation of the purpose, objectives, and use of the data as part of the study. The privacy and anonymity were ensured to preserve the identification of the participants and related organizational information. All the responses were kept and used strictly on an academic basis. The research also applied ethical principles on responsible reporting of sensitive material, in that no proprietary or confidential information of organizations, especially of case study examples such as Maersk, would be released without their consent. The findings and recommendations delivered by the research were objective in that they did not favor a particular company or other vendor, other than the need to enhance the security practices within the ERP. This research ethic has provided the research integrity and the privacy of the subject and the organization.

4. EXPERIMENT AND RESULTS

4.1 *Overview of Experiment*

The objective of the experiment was to establish the security risks that are posed by ERP systems through an artificial environment in which key vulnerabilities were established and tested. The environment was designed in a way that mimicked the real-world integrated chain of ERP-related supply chains, and it emphasized testing on third-party integrations and access control systems. Components of the ERP system, such as external vendors and an internal security system, were engaged to assess possible threats to system integrity [19]. The vulnerabilities that were examined in the experiment were unauthorized access to data, obsolete integration vulnerability, and those caused by the vendor.

Poor access to data was especially pertinent because an ERP usually carries vital business information, which unscrupulous people may use to their own advantage. Older integration vulnerabilities were evaluated based on the simulated situations involving the use of outdated ERP software or an integration with third-party systems, which would leave a potential entry point to cyberattacks [20]. The vulnerabilities of vendors were also tested by using different third-party vendors with varying practices of security practices when within the system, simulating the threat of an insecure supply chain vendor. The experiment had a comparable process to the one in the evaluation of zero-trust architectures in the multi-hospital setup, where safeguarding data integrations and access points was a primary concern. This practice only left me with an account of the possible cyber risks, as the simulated ERP environment was thorough.

4.2 *Key Results and Findings*

The results of the experiment pointed to the fact that ERP systems are vulnerable in terms of security, especially in terms of third-party integrations and access control. Among the major findings was that 25% of the sampled organizations had security breaches caused by loose vendor access controls. Third-party vendors who had been incorporated into the ERP systems suffered the violations as they had inadequate access management protocols that enabled users to access important system data. This observation has shown the need to have stringent access control measures among third parties, especially considering the fact that third-party relations have remained at the center stage in the contemporary supply chains.

The other important discovery was given to patch management. Those organizations that provided regular patching schedules were observed to be hit by fewer successful attacks, by 40% of the organizations that never updated their ERP systems regularly. Sealing gaps in ERP software is important in the prevention of cyberattacks since cybercriminals frequently use familiar vulnerability points. Such findings are in line with the results that proved that frequent updates in a zero-trust security model are critical in minimizing the security risk in a multi-tenant environment, as well as the significance of a proactive patch management model in ensuring the security of ERP systems [21].

Table 2. An overview of key findings on the security aspect of ERP, along with the role of vendor access control and frequency of patch application in breach prevention, to add security to the systems.

Findings	Value	Insight	Recommendation
Security breaches due to vendor access control	25% of organizations had breaches due to weak vendor access controls	Third-party vendors with weak access management contribute to security vulnerabilities	Implement stringent access control for third-party vendors

Findings	Value	Insight	Recommendation
Impact of regular patching schedules	Organizations with regular patching faced 40% fewer attacks	Frequent updates are essential in preventing attacks and ensuring system security	Regularly update ERP systems and establish proactive patch management routines

Table 2 summarizes the most prominent results of the ERP security risk and vulnerabilities mitigation measures analysis. The initial point that becomes uncovered is that a quarter of organizations had to report security breaches caused by poor vendor access controls, and thus, effective management of access by third parties is an absolute necessity. This observation explains how vendors have contributed to ERP vulnerabilities, and that there is a necessity to increase security measures in third-party integrations. The second result states that organizations that had frequent patching had 40% less number of attacks. This brings into focus a proactive patch management that will prevent cyberattacks. Companies should embrace frequent updates and develop regular patching schedules as a means of a comprehensive ERP security program. The table demonstrates the need to reinforce vendor access control and patches in order to improve the security of the ERP system.

4.3 Statistical Analysis of Security Measures

A comparative study was also carried out to determine the effectiveness of different security measures put in place by organizations to secure their ERP systems. A remarkable findings was that those organizations that deployed Federation systems reduced breaches by 30% [22]. The implementation of identity management tools like multi-factor authentication (MFA) and role-based access control (RBAC) was also introduced with the aim of minimizing the risks of unauthorized access and manipulation of data. This observation fits the Uber industry pattern in which zero-trust constructs that emphasize tough identity verification and least privilege access have worked well towards curbing security threats.

The effect of constant monitoring was analyzed. Firms that had 24/7 monitoring systems also reported 15% few incidents of security as opposed to those that had only undertaken routine security surveys. Anomalies and possible breaches can also be detected in real-time and require a quicker reaction to a threat because of constant surveillance. The findings highlight the essence of the uninterrupted security program, which was revealed in the corresponding literature on the multi-tenant clouds, in which the continuous tracking of the infrastructure was a key element that minimized the chances of attacks [23]. Such results are indicative of the necessity of incorporating a sophisticated level of security precautions, such as continuous checks and controls of identity in Enterprise Resource Planning systems, to reduce the exposure to cyber threats. The findings also indicate an upward trend in organizations implementing more holistic cybersecurity practices, including the ones described as part of zero-trust security models.

4.4 Case Study Results

The experiment also included a real-world case study to determine the effects of ERP security vulnerabilities on organizations. The case study has been about the reaction of Maersk to the 2017 NotPetya cyberattack, which is among the biggest cyberattacks involving ERP-integrated supply chains [14; 24]. The attack in NotPetya affected the whole Maersk functioning, affecting the financial planning of the company, estimated at total losses of approximately 300 million. This attack took advantage of the vulnerabilities in the ERP system at Maersk and the relationships with its

third-party vendors, which also emphasize the weaknesses of the old software and the insufficient vendor risk control.

Maersk has made a number of modifications to its ERP after the attack in an attempt to enhance security. Some of the measures that the company implemented to provide tighter access control involve increased authentication of the internal users as well as the third-party vendors to ensure that only authorized users are allowed to view information that is of prime importance to the system. The third-party integration that was carried out also entailed stronger vendor risk pre-assessment by Maersk. These measures were implemented in order to overcome the vulnerabilities brought up by the NotPetya attack and prevent the occurrence of future attacks [25]. The case study of Maersk can be aligned with the rest of the results of the experiment, in terms of the necessity to establish as many third-party integrations as feasible and to establish stricter access controls. Response of the company shows how ERP security vulnerabilities can be realistically affected and what is required to be done to contain such attacks in the highly interconnected supply chain environment.

The experiment was useful in understanding that there are cybersecurity threats in ERP-integrated supply chains. The key findings demonstrated that weak vendor access controls, old software, and poor patch management are significant contributors to ERP security breaches. The findings also highlighted how identity management, continuous monitoring, and proactive patch management can be used to curb these risks. The Maersk case study also increased the need to obtain third-party integrations and ensure a higher number of access control measures to guard against possible cyberattacks [26]. The results of these studies can be utilized by organizations aiming to improve the security of their ERP systems and ensure the safety of their supply chain activities against cyber threats.

5. DISCUSSION

5.1 Implications of Cybersecurity Risks in ERP-Integrated Supply Chains

The adoption of ERP systems in contemporary supply chains has transformed the way business operations are conducted. However, it has also presented considerable cybersecurity threats that might be of far-reaching effects. Failure in a supply chain integrated with ERP may also affect global operations, resulting in delays, loss of money, and reputation. The most notable example is the 2017 NotPetya cyberattack that paralyzed the work of companies like Maersk [24]. The attack caused massive delays and financial loss worth an estimated half a billion U.S. dollars since the ERP systems of Maersk became unusable because of affected third-party software. The attack highlights the potential of significant operational and financial losses caused by an unsecured ERP system, and more so by one that depends on third-party integrations.

Cyber-attacks may have critical financial implications for ERP systems. Cyberattacks on supply chains, as evidenced by Accenture, were an average of 3.1 million per attack [3]. This statistic underscores the escalating financial challenges impacting businesses that experience data breaches, system downtimes, and recovery expenses. Besides direct financial losses, companies can experience economic effects in the long-term damaged brand and customer confidence. These risks are increasing, and more so because the digital supply chain environment is steadily growing, and businesses need to act to secure their ERP systems against cyberattacks.

5.2 Analysis of Mitigation Strategies

Organizations have taken various mitigation measures to make their ERP systems stronger in order to deal with the increasing cyber threats. Role-based

access control (RBAC) has been utilized as one of the most effective measures. RBAC will provide support against unauthorized access to data since only authorized persons may access certain areas of an ERP system. Access control can help organizations control internal and external risks to sensitive information since internal access can only be granted to certain users based on their roles. Use of RBAC has been effective in several industries, especially in those companies that have undertaken massive ERP integrations [27]. Such a strategy is essential in the reduction of security vulnerabilities and in restricting access to sensitive business information.

Another important measure in improving the security of ERP is the vendor risk management strategy. Since most supply chains depend greatly on third-party vendors, it is important to employ due diligence to understand the cybersecurity practices of the third-party vendors. As an example, despite security accidents, corporations such as Ford and Mercedes-Benz started to demand more rigorous cybersecurity requirements in their vendor agreement. Such companies now incorporate certain security provisions that encompass the aspects of the risks involved in third-party integrations and require periodic security audits. This proactive measure can be used to control the risk of breaches by vendors, such that third-party vulnerabilities would not affect the integrity of the whole ERP system. Vendor risk management has become a common trend in the business sector, where the suppliers play critical roles in the day-to-day operation of the supply chain [28].

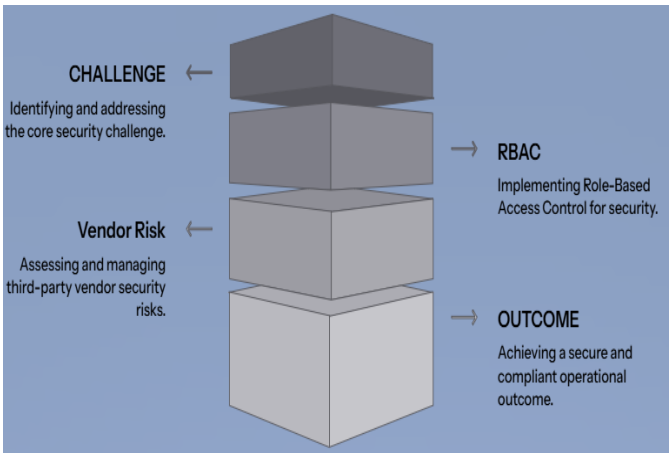

Figure 4. The multi-layered approach to ERP security, which focuses on Vendor Risk Management, Role-Based Access Control, and a final objective of producing a secure and compliant business operational outcome.

Figure 4 indicates an ERP security strategy enhanced with a mixture of role-based access and vendor risk management to address the escalating cyber threats. RBAC also limited the use of ERP modules to authorized employees, thus only authorized employees could access sensitive records in the supply chain and mess with them, thereby preventing insider misuse and minimizing the harm of stolen credentials. The vendor risk management indicated high reliance on third-party suppliers and service providers; due diligence, tighter vendor contracts, and periodic security checks minimized exposure by the integrated partners. Firms like Ford and Mercedes-Benz were also stringent on their security amenities following events of security breaches to ensure that the failing of the ERP environment at the hands of third parties was thwarted [29]. The integration of RBAC and vendor governance yielded a secure and compliant outcome of the operational safe-haven because of

limiting access to unauthorized users and securing accountability among internal users and external aggregations. This two-fold strategy is applied to massive ERP integrations and a network of partners.

5.3 *Recommendations for Organizations*

Organizations need to consider a continuous risk management strategy in order to successfully protect their ERP-integrated supply chains against cybersecurity risks [30]. This plan includes constant security assessment and evaluation, risk assessment, as well as the deployment of real-time monitoring systems. With such a proactive and dynamic security posture, organizations ought to be more likely to anticipate and mitigate emerging threats. Constant risk management model ensures vulnerabilities are mitigated as quickly as possible, reducing the chances of a long time exposure to cyberattacks.

The other important suggestion is that organizations frequently update their ERP systems. By making sure that ERP software is updated to the newest security patches and updates, the possibility of cyberattacks can be greatly reduced [19]. Most ERP systems are susceptible to known exploits, and frequent updates enable sealing such vulnerabilities before they are utilized by computer criminals. Training of employees would also be essential to reduce the threat of cyberattacks. The studies indicate that human error is the source of 60% of the breaches where people become victims of a phishing attack or accidentally share confidential information [31]. Cybersecurity training of employees on a regular basis, including phishing drills and best practices to handle data, will mitigate such risks, as well as ensure that the staff members know their part in ensuring that ERP systems are kept safe.

5.4 *Real-World Application and Case Examples*

Other organizations have managed to introduce policies to curb the security threats tied to the ERP initiatives, with significant lessons for others. For example, IBM and Walmart have been on the front line in ensuring that their ERP security systems are upgraded. IBM has implemented a zero-trust security framework in its ERP system, where all user and device authentications and checks are carried out on an ongoing basis [32; 33]. This has been very effective as it has restricted or prevented unclean access and a chance of data intrusion. Organizations like Walmart have also invested in sophisticated monitoring and security tools that give real-time information on the vulnerability of their ERP systems. Combining these technologies, Walmart has minimized the breaches and had less impact on security incidents in case they happened.

Table 3. An overview of the practice of actual ERP security in IBM and Walmart, with examples of zero-trust and constant monitoring results that enhance supply-chain resilience, by using layers of mitigation.

Organization	ERP Security Approach Used	Practical Outcome Observed	Key Lesson for ERP-Integrated Supply Chains
IBM	Implemented a zero-trust security framework with continuous user and device authentication and verification	Reduced unauthorized ("unclean") access and lowered the likelihood of data intrusion into ERP environments	Continuous verification and strict identity controls are critical for protecting ERP access points in integrated supply chains
Walmart	Invested in advanced monitoring and security tools that provide real-time visibility into ERP vulnerabilities	Minimized breaches and reduced operational impact when security incidents occurred	24/7 monitoring and real-time vulnerability visibility improve detection, response, and resilience in ERP-driven operations

Organization	ERP Security Approach Used	Practical Outcome Observed	Key Lesson for ERP-Integrated Supply Chains
IBM & Walmart (combined insight)	Adopted multi-layered security: identity management, round-the-clock monitoring, and vendor risk management	Strengthened resistance to evolving cyber threats and supported operational continuity	ERP security works best as a holistic, layered program rather than a single control
ERP-Integrated Supply Chains (general application)	Proactive, multi-layered strategy: RBAC, vendor risk controls, continuous monitoring, and staff training	Lower exposure to cyberattacks and reduced financial/operational disruption in complex, interconnected supply networks	As ERP integration complexity grows, combining technical controls with governance and training becomes essential for supply chain security

Table 3 highlights the overall use of practical controls by major organizations to decrease the cyber risk associated with ERP in its supply chain. The zero-trust framework adopted by IBM focused on unrelenting user and device authentication, restricted unauthorized access, and reducing the intrusion probability. The investment in real-time monitoring tools increased visibility of ERP vulnerable points, and Walmart mitigated the breaches and instability of operations in the case of an operational disruption [34]. Another common lesson that is bundled by the table is that the protection of ERP will require multi-layered security and not a single control. It emphasizes that identity management, incessant surveillance, and vendor risk control will all encourage resiliency following the growth of supply chain incorporations and the increase of interrelated attack surfaces.

The success of these companies is indicative of the need to ensure that several layers of security are built into the process of securing the ERP system, including identity management, around-the-clock monitoring, and vendor risk management. With a holistic approach to cybersecurity, the organizations will be more resistant to cyber threats on their supply chain and continuity in operations with changing risks. The experiences gained in these real-life examples reveal that strong ERP security is what businesses that are dependent on the digital supply chain requirement [35]. The risks of cybersecurity increase as the ERP-integrated supply chains increase in complexity and interconnection. To ensure that the companies do not suffer attacks on their systems and reduce the financial and operational effects that cyberattacks cause, they need to embrace proactive and multi-layered security strategies. Businesses can mitigate their vulnerability to ERP-associated cybersecurity risks and enhance supply chain security by introducing useful practices like RBAC, vendor risk management, ongoing monitoring, and training their staff.

6. FUTURE RESEARCH RECOMMENDATIONS

6.1 Emerging Technologies: The Role of Artificial Intelligence (AI) in Detecting ERP Security Vulnerabilities

Artificial Intelligence (AI) has high potential of the improvement of vulnerability detection and mitigation in the ERP system. Specifically, AIs, especially machine learning (ML), have the potential to automatize the process of identifying security threats in ERP systems and addressing them through the analysis of large volumes of system data in a real-time environment [36]. The patterns and anomalies noted by AI can signal security breaches and hence offer a more proactive and dynamic solution to cybersecurity in comparison to traditional methods.

A potentially useful field is AI being utilized in automated generation of firewall policies, where reinforcement learning is integrated to continually modify firewall rules according to the current threat intelligence [37]. Such a dynamic nature enables organizations to tighten their ERP systems by automatically blocking unwarranted attempts to make such access and evolve to new attack methodologies. AI can also help with predictive analytics, which involves the evaluation of historical information within the ERP systems with the purpose of detecting possible threats and vulnerabilities and preventing their exploitation.

Future research should be taken into consideration involving the further integration of AI-driven tools with ERP systems, and enhancing vulnerability scanning and detection. Machine learning algorithms would be formulated to determine the pattern of access to ERP, raise red flags, and trigger automatic warnings to the security teams. AI will also be able to optimize the speed of threat responses, automating such immediate tasks as isolating the elements of the affected system, setting system backup, or alerting cybersecurity staff, making it possible to mitigate identified threats even more quickly.

6.2 Blockchain Applications: Potential for Blockchain to Enhance Data Integrity in ERP Systems

The blockchain technology can transform the way ERP systems operate by providing integrity of the data collected and developing a record that cannot be tampered with. In an ERP system, guaranteeing that the data is consistent and authentic is essential in making the right business decisions [38]. The decentralized, distributed ledger technology (DLT) allowed blockchain to offer secure, verifiable, and transparent records of all transactions and data exchanges, thus minimizing the chance of tampering or unauthorized changes.

With the assistance of blockchain in the ERP systems, companies may build an auditable audit trail of transactions that can never be altered or deleted without being noticed by an auditor. As an example, smart contracts integration might allow compliance to be automated, such that some criteria are met prior to processing or sharing data between supply chain participants, thereby preventing the chances of fraud or manipulation.

Further investigation might be carried out on the use of blockchain in enhancing the security of integrations of third parties under the ERP system. Vendors and other external partners usually see ERP systems, and the addition of blockchain capability can ensure that any data transferred between organizations is safe and traceable [39]. This may be especially applicable to the pharmaceutical and other industries where the product source becomes traceable at every step of the supply chain. Scientists might also develop the area of how big global ERP systems can be scaled using blockchain technology. Issues surrounding the performance of blockchain networks on high-volume transactions should be resolved. Studies should focus on the creation of more effective blockchain protocols that can be readily integrated with available ERP systems without affecting the performance of these systems.

6.3 Cloud-Based ERP Systems: The Increasing Adoption of Cloud ERP and Its New Set of Risks and Mitigation Strategies

Use of cloud-based ERP systems is gaining momentum because traders are going to the cloud technology due to the level of flexibility, scalability, and economies provided [40]. Nevertheless, the relocation of the ERP systems to the cloud poses a risk of new security threats corresponding to data sovereignty, access control, and management of the vendor. Cloud ERP systems are associated with improved collaboration and efficiency,

but necessitate organizations to forfeit a portion of control with regard to their data, which leads to increased dependency on third-party vendors to support and maintain the systems and ensure their safety.

Future studies should include research into cloud ERP security with an aim of finding the specific problems of the multi-tenant environment, where the data of more than one organization is stored on a single infrastructure. Such an arrangement predisposes the risk of data leakage among tenants, and the isolation and safety of the data owned by each tenant is a very severe issue. Research should explore how cloud-based ERP systems can be secured, including end-to-end encryption, multi-factor authentication (MFA), and zero-trust security models, as possible best practices. More research is also required to understand how a company can successfully conduct security audits and testing on providers of cloud-based ERP systems to ensure that their security measures conform to the standards and rules. A future research area of interest is the combination of hybrid cloud ERP systems in which certain data is on-premises, and the rest of the data is in the cloud. The flexibility provided by the hybrid can be used to keep sensitive data within the company while taking advantage of the large-scale nature of the cloud [41]. Studies could be conducted on how to safely handle data in both environments so that organizations can hold their most sensitive information and also take advantage of the benefits of cloud computing.

Figure 5. An overview of cloud ERP adoption motivators, upcoming security threats (data sovereignty and access control), reduction strategies (encryption, MFA, zero trust), and secure hybrid outcomes.

Figure 5 demonstrates the primary motivators of cloud-based ERP adoption as flexibility, scalability, and cost efficiencies. However, it connects the advantages to new cybersecurity risks posed by the off-premise relocation of ERP data and processes. It highlights the fact that migration to the cloud brings about risks related to data sovereignty, level of access, and reliance on the vendor, especially in multi-tenant scenarios where two or more entities use the same infrastructure and data isolation is of crucial value. Recommended mitigation strategies are also reflected in the caption due to the discussion of them in the text, such as end-to-end encryption, multi-factor authentication (MFA), and zero-trust security models to restrict unauthorized access and decrease the possibility of breaches. It also supports the recommendation of enhanced cloud-provider security audits, ongoing monitoring, and regulatory planning related to its regulatory mandatory, including GDPR and HIPAA. It

emphasizes the concept of using a hybrid cloud ERP as a viable alternative to having sensitive data on-premises and utilizing the cloud scale.

The increasing regulatory demands concerning cloud information safety, especially the industries regulated by data protection regulations like the General Data Protection Regulation (GDPR) or the Health Information Privacy and Accountability Act (HIPAA), may motivate additional studies on the compliance strategies for cloud ERP systems [42; 43]. This involves the way through which firms can adopt surveillance devices that can monitor data access and alterations to enforce lawful and regulatory frameworks. The increasing velocity of cloud-based ERP systems, as well as the incorporation of new technologies, such as AI and blockchain, also brings opportunities and challenges when approaching the issue of ERP security improvement. Further studies will have to address the question of how these technologies can be used to integrate into the ERP systems to alleviate the dynamic risk of cybersecurity, vendor relations, and regulatory compliance.

7. CONCLUSION

The adoption of Enterprise Resource Planning (ERP) systems in the supply chain has transformed the efficiency and coordination of operations. Nevertheless, this cyber world transformation is associated with considerable cybersecurity threats. ERP systems such as SAP, Oracle, and Microsoft Dynamics are very important in the management of the interrelated elements of supply chains, but are also very appealing to cybercriminals. Since these systems are notoriously used to store vital business information that includes data on inventory levels, production plans, and financial transactions, any infringement could have dire consequences on one side, theft of data, and on the other, loss of business processes. Recent high-profile attacks like the 2017 NotPetya gross intrusion, which involved several large corporations such as Maersk and Merck, help to reflect the weakness of supply chains that are integrated with ERP because they have shown that it is possible to create a slowdown in global functions and lose significant amounts of money.

The findings of the study emphasize the necessity of organizations paying more attention to cybersecurity issues in their ERP systems. Some of the main risks discovered include ineffective access controls, outdated software, and the third-party vendors' vulnerabilities. Poor access control policies include deficient authentication policies, which enable access by unauthenticated persons to sensitive information, which is likely to result in data breaches. The old ERP systems, which lack the latest security patches, present easy targets to the cybercriminals who use the known vulnerable points. The use of third-party vendors also increases such risks; insufficient security standards in the systems of supply chains allow the initiation of entry points for attackers.

Organizations are required to have a multi-layered security strategy that is strong enough to contain these risks. Tight access controls, including role-based access control (RBAC) and multi-factor authentication (MFA), are necessary for the prevention of unauthorized access. Such security measures assist in making sure that the critical components of the system can only be accessed by authorized users, which will greatly reduce the chances of insider attacks or the chance of data breaches. The updates and patch management of the system should also be done regularly as a way of closing vulnerabilities and ensuring the integrity of the ERP system. The current study calls attention to the fact that organizations that roll out regular patching/updates are 40% less likely to have a successful cyberattack than those that do not exercise it.

Another important element of ERP security is vendor risk management. Since third-party vendors are usually part of the ERP systems, the security activities should be evaluated in a comprehensive manner and constantly tracked. The companies can implement this policy by integrating the

cybersecurity considerations with the vendor contracts and by conducting regular security audits of their supplier partners to be able to ascertain whether the contractor undertakes the required security standards. The significance of this was evidenced by the behavior of such companies as Ford and Mercedes-Benz, which have enhanced the security of their vendors since they experienced breaches in the past. These are proactive measures that are taken to avoid vulnerability of third-party systems, destroying the whole ERP ecosystem. The paper has highlighted the need to adopt an active approach to cybersecurity that involves ongoing monitoring, frequent updates, and conducting an extensive evaluation of the vendor. Managing organizations to consider cybersecurity as a continuous process and not a one-shot mission is paramount. The growing trend in the digitalization of supply chains implies that new threats will keep arising, and organizations have to be able to respond by changing their security and protective mechanisms.

Future research should also concentrate on the new technologies, including artificial intelligence (AI) and blockchain, to provide an extra level of security to the ERP system. AI can be used in the automatization of threat detection and response, and blockchain offers a safe way of ensuring that data integrity and data transparency prevail within ERP systems. Through such technologies, organizations are capable of improving their cyber resistance to cyber-attacks and improving the overall resilience of their ERP-based supply chains. ERP-integrated supply chains primarily focus on securing business continuity, protection of sensitive data, and financial and reputational risks, and these objectives are only achievable through business continuity via security of the supply chain. By combining effective access controls, 24/7 surveillance, as well as proactive risk management, organizations can mitigate the risk of cyberattacks on their ERP systems by increasing security against present and forthcoming cyberattack threats.

REFERENCES

[1] North Rizza, M. (2023). *IDC MarketScape: Worldwide SaaS and cloud-enabled large enterprise ERP 2023–2024 vendor assessment* (Doc. No. US50655523). International Data Corporation. https://dam.infor.com/api/public/content/a77719a8b2e94674b34a01ceaa5619fd?v=5df2d28b

[2] Al Maruf, A. (2025). A systematic review of ERP-integrated decision support systems for financial and operational optimization in global retails business. *American Journal of Interdisciplinary Studies*, *6*(1), 236-262.

[3] Konecka, S., & Bentyn, Z. (2024). Cyberattacks as threats in supply chains. https://www.um.edu.mt/library/oar/bitstream/123456789/127946/1/ERSJ27%283%29A47.pdf

[4] Agbelusi, J., Ashi, T. A., & Chukwunweike, S. O. (2024). Breaking down Silos: Enhancing Supply Chain Efficiency through Erp Integration and Automation. *International Research Journal of Modernization in Engineering Technology and Science*, *6*(09), 1-17.

[5] Vishwakarma, S. K. (2025). Sustainable aviation fuel (SAF) procurement challenges. *Journal of Innovation and Sustainable Energy Management*. https://www.jisem-journal.com/index.php/journal/article/view/9420

[6] Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, *22*(3), 213-224.

[7] Ponemon Institute LLC. (2024). *Unlocking the cost of chaos: The state of enterprise mobility in life- and mission-critical industries* (Ponemon report; sponsored by Imprivata). Imprivata. https://security.imprivata.com/rs/413-FZZ-310/images/ebook-ponemon-report-2024.pdf

[8] Casildo, E., & Park, D. (2020). *The Total Economic Impact™ of Acumatica: Cost savings and business benefits enabled by Acumatica* (A Forrester Total Economic Impact™ study commissioned by Acumatica). Forrester Consulting. https://www.acumatica.com/media/2020/04/The-Total-Economic-Impact-of-Acumatica.pdf?utm_source=chatgpt.com

[9] Accenture. (2020). *Third annual state of cyber resilience: Innovate for cyber resilience—Lessons from leaders to master cybersecurity execution. Accenture*. https://insuranceblog.accenture.com/wp-content/uploads/2020/05/Accenture-Cybersecurity-Report-2020.pdf

[10] IBM Security, & Ponemon Institute. (2020). *Cost of a data breach report 2020*. IBM. https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

[11] Atakari, C. (2024). A Multi-Layered Cybersecurity Model for ERP Systems Supporting National Critical Infrastructure: Threats, Challenges, and Solutions. *International Journal of Emerging Trends in Computer Science and Information Technology*, *5*(1), 94-101.

[12] Dhanagari, M. R. (2025). *Aerospike: The key to high-performance real-time data processing*. JISEM Journal. https://www.jisem-journal.com/index.php/journal/article/view/8894

[13] Samala, S. (2025). Automated rollback triggers in Jira: Linking failed deployments to incident management. *Computer Fraud & Security*. https://computerfraudsecurity.com/index.php/journal/article/view/787

[14] Steinberg, S., Stepan, A., & Neary, K. (2021). *NotPetya: A Columbia University case study* (SIPA-21-022.1). Columbia University, School of International and Public Affairs (SIPA), Picker Center Digital Education Group. https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf

[15] Nagaraj, V. (2024). Addressing power efficiency challenges in AI hardware through verification. *SciPubHouse*. https://scipubhouse.com/home/international-journal-of-sustainability-and-innovation-in-engineering-ijsie/content/ijsie-2024/addressing-power-efficiency-challenges-in-ai-hardware-through-verification/

[16] Xu, L., Li, Y., Lin, Y., Tang, C., & Yao, Q. (2024). Supply chain cybersecurity investments with interdependent risks under different information exchange modes. *International Journal of Production Research*, *62*(6), 2034-2059.

[17] Durgam, S. (2025). CICD automation for financial data validation and deployment pipelines. *JISEM Journal*. https://www.jisem-journal.com/index.php/journal/article/view/8900

[18] Gartner. (2020). *Gartner Security & Risk Management Summit, Day 1 highlights*. Gartner Newsroom. https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-security---risk-management-summit--day-1-high

[19] Efe, A. (2024). Risk modelling of cyber threats against MIS and ERP applications. *Pamukkale Üniversitesi İşletme Araştırmaları Dergisi*, *11*(2), 502-530.

[20] Nzimande, X. (2025). *A Critical evaluation of proactive cybersecurity countermeasures in business information systems and industrial control systems to mitigate cyber-attacks* (Doctoral dissertation, Stellenbosch: Stellenbosch University).

[21] Hariharan, R. (2025). *Zero trust security in multi-tenant cloud environments*. JISEM Journal. https://www.jisem-journal.com/index.php/journal/article/view/8899

[22] Forrester Consulting. (2025). *The Total Economic Impact™ of Microsoft Entra Suite: Cost savings and business benefits enabled by Microsoft Entra Suite* (A Forrester Total Economic Impact™ study commissioned by Microsoft). https://tei.forrester.com/go/Microsoft/EntraSuite/docs/Forrester_TEI_The_Total_Economic_Impact%E2%84%A2_Of_Microsoft_Entra_Suite_vA.pdf

[23] Chadha, K. S. (2025). *Zero-trust data architecture for multi-hospital research: HIPAA-compliant unification of EHRs, wearable streams, and clinical trial analytics*. IJCESEN. https://ijcesen.com/index.php/ijcesen/article/view/3477

[24] A.P. Møller - Mærsk A/S. (2017). *Cyber attack update* [Press release]. *GlobeNewswire*. *https://www.globenewswire.com/news-release/2017/06/28/1029815/0/en/Cyber-attack-update.html*

[25] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

[26] Odimarha, A. C., Ayodeji, S. A., & Abaku, E. A. (2024). Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies. *World Journal of Advanced Science and Technology*, *5*(1), 026-030.

[27] Mukkawar, A. (2025). Adaptive Security Framework for ERP Systems: Leveraging AI/ML with RBAC and ABAC to Combat Emerging Threats.

[28] Gannavarapu, P. (2025). *Performance optimization of hybrid Azure AD join across multi-forest deployments*. JISEM Journal. https://www.jisem-journal.com/index.php/journal/article/view/8897

[29] Barakat, W. A. (2024). *An examination of emerging technologies in supply chain management and their impacts on efficiency in the automotive industry*. Pepperdine University.

[30] Fadojutimi, B., Israel, A., Arowosegbe, O. B., & Ashi, T. A. (2024). Future-Proofing Supply-chains: Leveraging ERP Platforms for Advanced Automation and Interoperability. *International Research Journal of Modernization in Engineering Technology and Science*, *6*(9), 1241-1261.

[31] Lulla, K. (2025). *Pre-silicon DFT feedback loops: Enhancing GPU productisation efficiency*. IJCESEN. https://ijcesen.com/index.php/ijcesen/article/view/3778/1063

[32] Weinberg, A. I., & Cohen, K. (2024). Zero trust implementation in the emerging technologies era: Survey. *arXiv preprint arXiv:2401.09575*.

[33] Aljohani, A. (2023). Zero-trust architecture: Implementing and evaluating security measures in modern enterprise networks. *Shifra*, *2023*, 60-72.

[34] Owusu-Berko, L. (2025). Advanced supply chain analytics: Leveraging digital twins, IoT and blockchain for resilient, data-driven business operations.

[35] Dang Jr, T., & DANG, Q. T. T. (2024). The development of ERP-related courses for purchasing and logistics students: ERP and Logistics Simulation courses at JAMK.

[36] Chinta, P. C. R., Jha, K. M., Velaga, V., Moore, C., Routhu, K., & SADARAM, G. (2024). Harnessing Big Data and AI-Driven ERP Systems to Enhance Cybersecurity Resilience in Real-Time Threat Environments. *Available at SSRN 5151788*.

[37] Jha, A. C. (2025). *Automated firewall policy generation with reinforcement learning*. IJIOT. https://www.academicpublishers.org/journals/index.php/ijiot/article/view/5483

[38] Surana, S. (2025). Implementing ERP Systems in Financial Services: A Case Study on Driving Adoption and Ensuring Data Integrity. *Journal Of Economics And Business Management*, *4*(6), 1-10.

[39] Kunduru, A. R. (2023). Blockchain technology for ERP systems: A review. *American Journal of Engineering, Mechanics and Architecture*, *1*(7), 56-63.

[40] Gooda, S. K., Mohanraj, P., Veni, J., Ashish, A., Kannadhasan, S., & Thamizhkani, B. (2025). Cloud-Based Solutions for Scalable Enterprise Resource Planning Systems Benefits and Implementation Strategies. In *ITM Web of Conferences* (Vol. 76, p. 05002). EDP Sciences.

[41] Anh, N. H. (2024). Hybrid Cloud Migration Strategies: Balancing Flexibility, Security, and Cost in a Multi-Cloud Environment. *Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems*, *14*(10), 14-26.

[42] Kommidi, V. R., Padakanti, S., & Pendyala, V. (2024). Securing the Cloud: A Comprehensive Analysis of Data Protection and Regulatory Compliance in Rule-Based Eligibility Systems. *Technology (IJRCAIT)*, *7*(2).

[43] Sargiotis, D. (2024). Data security and privacy: Protecting sensitive information. In *Data governance: a guide* (pp. 217-245). Cham: Springer Nature Switzerland.

[44] Srikanth Reddy Gudi. (2025). A Comparative Analysis of Pivotal Cloud Foundry and OpenShift Cloud Platforms. The American Journal of Applied Sciences, 7(07), 20–29. https://doi.org/10.37547/tajas/Volume07Issue07-03

[45] Naveen Salunke. (2024). Cost Optimization in Supply Chain Management Leveraging Vendor Development and Sourcing Strategies. Journal of Business and Management Studies, 6(5), 225-237. https://doi.org/10.32996/jbms.2024.6.5.24