Cilt: 11 Sayı:2, 2024, ss. 502-530

PAMUKKALE ÜNİVERSİTESİ
İŞLETME ARAŞTIRMALARI DERGİSİ (PIAR)
Pamukkale University Journal of Business Research
https://dergipark.org.tr/tr/pub/piar

Risk Modelling of Cyber Threats Against MIS and ERP Applications

MIS ve ERP Uygulamalarına Yönelik Siber Tehditlerin Risk Modellemesi

Ahmet EFE [1*]

[1] International Federation of Red Cross and Red Crescent, icsiacag@gmail.com, ORCID: 0000-0002-2691-7517
* Yazışılan Yazar/Corresponding author

Makale Geliş/Received: 16.09.2024 Makale Kabul/Accepted: 24.12.2024

Araştırma Makalesi / Research Paper DOI: 10.47097/piar.1550812

Abstract

This study presents a detailed examination of cyber threats impacting Management Information Systems (MIS) and Enterprise Resource Planning (ERP) applications. It explores various types of cyber threats, such as malware, ransomware, phishing, insider threats, DDoS attacks, zero-day exploits, and Advanced Persistent Threats (APTs), assessing their potential impacts on businesses. The study introduces a novel risk modeling approach to quantify these threats by evaluating their threat levels, impacts, and probabilities of occurrence, providing a comprehensive risk score. Emphasizing the importance of proactive measures, advanced security technologies, and a strong organizational culture, the study highlights how these elements are crucial for effective cybersecurity. By integrating these strategies and continuously updating security measures, businesses can better protect their critical systems and mitigate the risks posed by evolving cyber threats.

Keywords: *Cybersecurity, MIS, ERP, Cyber Threats, Mitigation Strategies, Risk Modelling.*

Jel Codes: *D81, L86, M15, G32, O33.*

Öz

Bu çalışma, Yönetim Bilişim Sistemleri (MIS) ve Kurumsal Kaynak Planlama (ERP) uygulamalarını etkileyen siber tehditlerin ayrıntılı bir incelemesini sunmaktadır. Çalışmada, zararlı yazılımlar, fidye yazılımları, oltalama saldırıları, iç tehditler, DDoS saldırıları, sıfırıncı gün açıkları ve Gelişmiş Kalıcı Tehditler (APT'ler) gibi çeşitli siber tehdit türleri ele alınarak, bunların işletmeler üzerindeki olası etkileri değerlendirilmektedir. Çalışma, bu tehditlerin seviyelerini, etkilerini ve ortaya çıkma olasılıklarını değerlendirerek tehditlerin nicel olarak ölçülmesine olanak tanıyan yeni bir risk modelleme yaklaşımı sunmakta ve kapsamlı bir risk skoru sağlamaktadır. Proaktif önlemlerin, ileri güvenlik teknolojilerinin ve güçlü bir örgütsel kültürün önemine vurgu yapan bu çalışma, etkili bir siber güvenlik için bu unsurların kritik olduğunu öne çıkarmaktadır. Bu stratejilerin entegrasyonu ve güvenlik önlemlerinin sürekli güncellenmesiyle, işletmeler kritik sistemlerini daha iyi koruyabilir ve gelişen siber tehditlere karşı riskleri azaltabilir.

Anahtar Kelimeler: *Siber Güvenlik, MIS, ERP, Siber Tehditler, Risk Azaltma Stratejileri, Risk Modelleme.*

Jel Kodları: *D81, L86, M15, G32, O33.*

Atıf için (Cite as): Efe, A. (2024). Risk modelling of cyber threats against MIS and ERP applications. *Pamukkale Üniversitesi İşletme Araştırmaları Dergisi, 11*(2), 502-530. https://doi.org/10.47097/piar.1550812

1. INTRODUCTION

In today's digital era, MIS and ERP applications serve as the operational core of organizations, enabling efficient resource management, streamlined processes, and informed strategic decision-making. However, the increasing complexity and sophistication of cyber threats pose a growing risk to the integrity and functionality of these critical systems. This study presents an examination of these vulnerabilities, focusing on risk modelling of the ever-evolving threat landscape and its profound implications for businesses. By exploring the intricate nature of cyber threats such as malware, ransomware, phishing, and advanced persistent threats (APTs), the study underscores the pressing need for robust, multi-layered cybersecurity measures to safeguard these essential platforms.

1.1. Research Design

The research employs a mixed-methods approach, integrating both qualitative and quantitative data to offer a comprehensive analysis of the cyber threats targeting MIS and ERP applications. The research progresses through two key phases:

1. Literature Review: A detailed review of existing literature forms the theoretical foundation, identifying common cyber threats and vulnerabilities within MIS and ERP applications. Synthesizing insights from previous studies, industry reports, and cybersecurity white papers, this phase establishes a comprehensive understanding of the current threat landscape.

2. Risk Modelling: The study develops a risk modeling formula that incorporates the varying severity and probability of different cyber threats. This model facilitates the prioritization of vulnerabilities and the formulation of tailored security strategies. This study significantly contributes to the cybersecurity literature by addressing a notable gap in existing research—while numerous studies have explored the nature and impact of cyber threats on MIS and ERP applications, no prior research has focused on risk modeling or formulating risk scores specific to these systems. By introducing a novel approach to quantify cyber threats through evaluating threat levels, impacts, and probabilities, this research provides a comprehensive risk modeling framework. This advancement enables organizations to prioritize vulnerabilities and design tailored security strategies, filling a critical void in current cybersecurity studies.

1.2. Hypothesis

The central hypothesis of this study posits that the increasingly sophisticated and damaging cyber threats targeting MIS and ERP applications can be effectively analyzed through risk modeling, which enables the development of advanced, multi-layered security measures. Specifically, the study suggests that organizations with proactive cybersecurity strategies and comprehensive security policies experience fewer and less severe breaches compared to those employing reactive or inadequate approaches.

1.3. Assumptions

This research rests on several key assumptions:

1. Evolution of Threats: The study assumes that cyber threats are continuously evolving, with attackers employing more advanced techniques to exploit MIS and ERP vulnerabilities.

2. Impact of Threats: It is assumed that cyber threats have a significant impact on MIS and ERP applications, potentially disrupting operations, causing financial losses, damaging reputations, and incurring regulatory penalties.

3. Mitigation Strategies: The study presupposes that proactive mitigation strategies—such as continuous monitoring, employee training, and the implementation of robust security frameworks—can significantly reduce both the likelihood and severity of cyber incidents.

4. Data Accuracy: The study assumes that the data sourced from incident reports, threat intelligence, and expert interviews is accurate and reflective of the broader cybersecurity environment.

1.4. Limitations

While comprehensive, the study acknowledges several limitations:

1. Data Availability: Access to detailed incident data may be limited due to confidentiality and proprietary concerns, potentially affecting the depth of the analysis.

2. Technological Changes: Rapid advances in cybersecurity threats and solutions may reduce the long-term applicability of the study's findings as new threats and defense mechanisms emerge.

By addressing these aspects, this study contributes valuable insights into the field of cybersecurity, offering practical recommendations for enhancing the resilience of MIS and ERP applications through advanced risk modeling and proactive security measures.

2. BACKGROUND ON MIS AND ERP APPLICATIONS

MIS and ERP applications are integral components of modern organizational infrastructure. They serve distinct yet overlapping roles in managing and optimizing business processes. This section provides a detailed overview of these systems, their types, emerging trends, and the impact of cloud computing and artificial intelligence (AI) on their evolution.

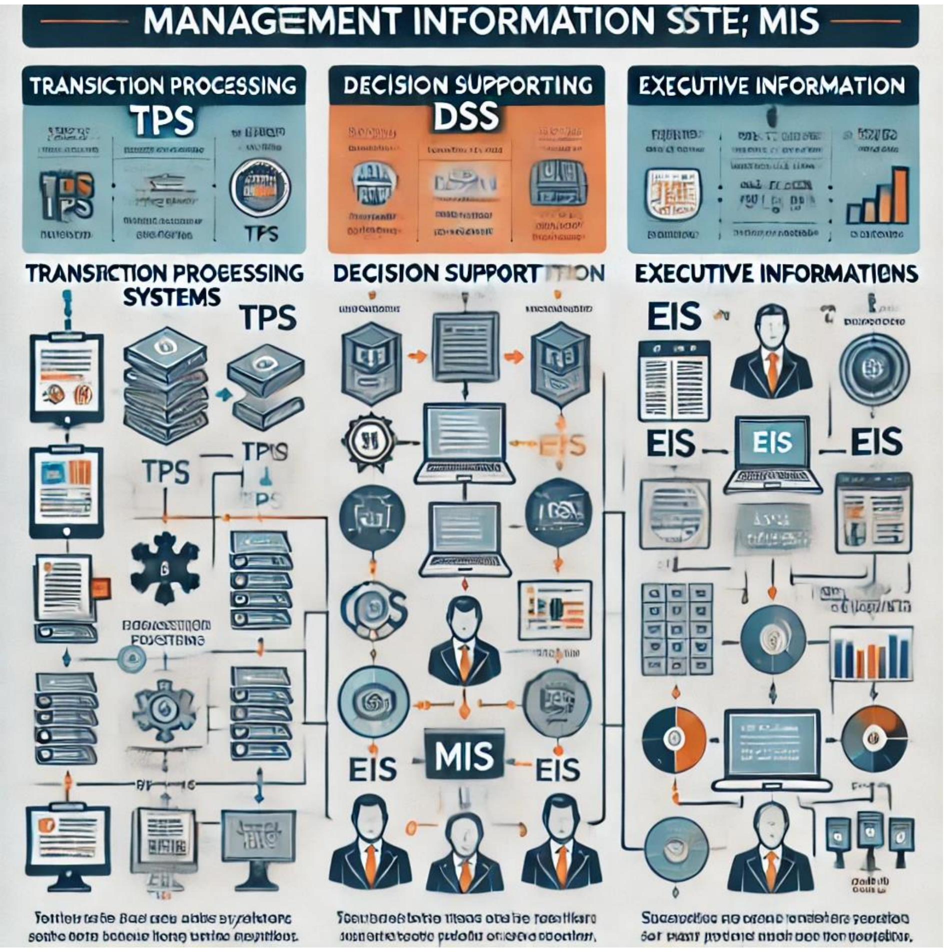

Figure 1. Depiction of MIS components

Source: Developed by author using AI

2.1. Management Information Systems (MIS)

MIS are designed to support managerial decision-making by providing timely, relevant, and accurate information. MIS encompass a broad range of systems used to manage organizational data, including transaction processing systems, decision support systems, and executive information systems (Laudon & Laudon, 2020). The primary types of MIS include:

- Transaction Processing Systems (TPS): These systems handle daily transactions and routine operations, such as order processing, payroll, and inventory management (Rahmatian, 2002).

- Decision Support Systems (DSS): DSS assist in complex decision-making processes by analyzing data and generating reports that support managerial decisions (Marakas 2003).

- Executive Information Systems (EIS): EIS provide top executives with summarized reports and critical metrics to aid strategic planning and performance monitoring (Leidner, 1993).

2.2. Enterprise Resource Planning (ERP) Applications

ERP systems are comprehensive software solutions designed to integrate and streamline business processes across an organization.

Figure 2. Simple depiction of ERP

Source: Developed by author using AI

ERP facilitate real-time data sharing and coordination among various departments, improving efficiency and decision-making. Key types of ERP modules include:

- Financial Management: Manages financial transactions, accounting, and reporting (Monk & Colmenares, 2009).

- Human Resources Management: Handles employee data, payroll, and performance management (Alhalboosi, 2021).

- Supply Chain Management: Oversees procurement, inventory, and logistics operations (Choudhuri, 2024).

- Customer Relationship Management (CRM): Manages customer interactions, sales, and support (AlJawarneh & Al-Omari, 2018).

2.3. Trends in Cloud Computing

The advent of cloud computing has significantly impacted MIS and ERP applications. Cloud-based solutions offer several advantages, including scalability, cost efficiency, and accessibility.

Figure 3. Simple depiction of Cloud systems

Source: Developed by author using AI

Cloud platforms such as Microsoft Azure, Amazon Web Services (AWS), and Google Cloud provide robust environments for hosting and managing MIS and ERP applications. Key trends include:

- Adoption of SaaS (Software as a Service): Organizations increasingly prefer SaaS ERP solutions for their flexibility and lower upfront costs (Walko et al, 2020).

- Integration with IoT (Internet of Things): Cloud-based ERP systems are integrating with IoT devices to enhance real-time data collection and process automation (Hassan et al, 2024).

- Enhanced Security Measures: Cloud providers are investing in advanced security features to protect data and comply with regulatory standards (Adeusi, 2024).

2.4. Impact of Artificial Intelligence (AI) Algorithms on Cyber Landscape

AI algorithms are transforming MIS and ERP applications by enhancing their capabilities and introducing new functionalities. AI applications include:

- Predictive Analytics: AI algorithms analyze historical data to forecast trends and support strategic planning (Ajiga, 2024).

- Automated Decision-Making: AI-driven systems can automate routine tasks and decision processes, improving efficiency (Badmus et al, 2024).

- Natural Language Processing (NLP): NLP technologies enable better interaction with ERP systems through voice commands and text analysis (Malik & Bilal, 2024).

Overall, the integration of cloud computing and AI into MIS and ERP applications reflects a broader trend towards more agile, intelligent, and interconnected business environments.

3. IMPORTANCE OF CYBERSECURITY FOR MIS AND ERP APPLICATIONS

The significance of cybersecurity in the realm of MIS and ERP applications cannot be overstated. These systems are integral to the operational framework of modern organizations, handling critical data and processes that are fundamental to business operations. As such, ensuring their security is paramount to protect against an array of cyber threats that can have devastating effects.

The shift towards cloud-based solutions and the incorporation of artificial intelligence (AI) algorithms in MIS and ERP applications introduces both opportunities and vulnerabilities:

- Cloud Security Challenges: While cloud computing offers scalability and flexibility, it also presents unique security challenges. Misconfigurations, insufficient access controls, and shared infrastructure vulnerabilities are prominent concerns. Recent studies have highlighted that misconfigured cloud storage can lead to data breaches and exposure of sensitive information (Alquwayzani et al, 2024).

- AI and Machine Learning: AI algorithms are increasingly used for threat detection and response, offering enhanced capabilities to identify and mitigate cyber threats. However, the same technology can be leveraged by attackers to develop sophisticated attacks. Adversarial machine learning, for example, involves manipulating AI systems to bypass security measures or generate false positives (Thomas, 2020).

- Zero Trust Architecture: The adoption of Zero Trust principles is becoming a trend in securing cloud and AI-integrated systems. Zero Trust assumes that threats could be internal or external, and thus, it mandates continuous verification of users and devices regardless of their location (Ahmadi, 2024).

The importance of cybersecurity for MIS and ERP applications is underscored by the diverse range of cyber threats and the evolving landscape of cloud and AI technologies. Proactive measures, robust security policies, and staying abreast of emerging trends are crucial in safeguarding these critical systems. As cyber threats become more sophisticated, a comprehensive and dynamic approach to cybersecurity is essential to protect the integrity and confidentiality of MIS and ERP applications.

4. TYPES OF CYBER THREATS

As organizations increasingly rely on MIS and ERP applications to manage their operations and data, they become prime targets for a diverse array of cyber threats. Among these, malware threats pose significant risks by maliciously infiltrating systems to damage or steal data. Ransomware threats further exacerbate the danger by encrypting critical files and demanding ransom for their release, often crippling operations in the process. Phishing and social engineering attacks exploit human vulnerabilities to gain unauthorized access, while insider threats involve malicious or negligent actions by trusted employees who compromise security from within. Distributed Denial of Service (DDoS) attacks overwhelm systems with excessive traffic, leading to service disruptions. Zero-day exploits target unpatched vulnerabilities in software, presenting significant challenges due to their sudden and unexpected nature. Finally, Advanced Persistent Threats (APTs) represent a sophisticated form of cyber intrusion where attackers maintain a prolonged presence in a network to exfiltrate data and undermine security. Understanding these threats is crucial for developing effective strategies to safeguard MIS and ERP applications against an ever-evolving cybersecurity landscape.

4.1. Malware Threat

Malware represents one of the most significant and persistent threats to MIS and ERP applications. This section explores the nature of malware threats, their impact on MIS and ERP applications, and effective strategies for mitigation.

Malware, short for malicious software, is designed to infiltrate, damage, or exploit computer systems and networks. It encompasses various types, each with unique characteristics and methods of attack. The principal types include:

- Viruses: Self-replicating malware that attaches to legitimate files and spreads through systems, often leading to data corruption and system malfunction (McAfee, 2023).

- Worms: Independent programs that spread across networks without human intervention, exploiting vulnerabilities to propagate and potentially cause widespread damage (Symantec, 2022).

- Trojan Horses: Malware disguised as legitimate software, which, once installed, gives attackers unauthorized access to the system (Kaspersky, 2024).

- Ransomware: A type of malware that encrypts data and demands a ransom for decryption keys, disrupting business operations and potentially causing significant financial losses (ESET, 2024).

- Spyware: Software that secretly monitors and collects user data, compromising privacy and potentially leading to data breaches (Palo Alto Networks, 2023).

The impact of malware on MIS and ERP applications can be profound, affecting both operational integrity and business continuity:

1. Data Integrity and Confidentiality: Malware can corrupt or steal sensitive data, undermining the integrity and confidentiality of critical business information. This can result in financial losses, reputational damage, and legal repercussions (IBM, 2023).

2. Operational Disruption: The presence of malware can lead to system outages, slowed performance, and overall operational disruption. In ERP systems, this can affect various functions, from inventory management to financial reporting, causing significant business interruptions (FireEye, 2024).

3. Financial Losses: The direct and indirect costs associated with malware attacks, including ransom payments, remediation efforts, and loss of productivity, can be substantial.

Additionally, the long-term financial impact includes increased insurance premiums and potential regulatory fines (Cisco, 2023).

4.2. Ransomware Threat

Ransomware represents a significant and evolving threat to MIS and ERP applications. This form of cyber-attack involves malicious actors encrypting a victim's data, rendering it inaccessible until a ransom is paid. The impact of ransomware on MIS and ERP applications can be devastating, affecting business operations, financial stability, and data integrity.

Ransomware attacks are typically executed through phishing emails, malicious downloads, or vulnerabilities in software (Nagar, 2024). The ransomware encrypts files on the infected system and demands a ransom, often in cryptocurrency, for the decryption key. Modern ransomware variants have become increasingly sophisticated, employing techniques such as double extortion, where attackers not only encrypt data but also threaten to release it publicly if the ransom is not paid (Sharmeen, 2020).

The consequences of a ransomware attack on MIS and ERP applications are profound. These systems are integral to managing a company's operations, financial data, and strategic planning. The encryption of data can halt business processes, disrupt operations, and cause significant financial losses. In addition to direct operational impacts, the loss of data integrity can compromise decision-making and strategic planning, leading to long-term repercussions for the organization’s competitiveness and reputation (Malik et al, 2022).

Ransomware attacks can also result in legal and regulatory consequences. Organizations may face compliance issues, particularly if they handle sensitive data subject to regulations such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA) (Shaikh et al., 2024). The inability to access or protect data as required by these regulations can lead to fines and legal actions, further exacerbating the financial and reputational damage.

Historically, ransomware has evolved from relatively simple encryption schemes to complex and highly effective attacks targeting enterprise environments. Early ransomware variants were rudimentary, often relying on straightforward encryption algorithms and basic social engineering techniques (SANS Institute, 2023). In contrast, contemporary ransomware employs advanced encryption techniques and sophisticated distribution methods, including exploitation of zero-day vulnerabilities and integration with ransomware-as-a-service (RaaS) platforms, which lower the barrier to entry for cybercriminals (Alwashali et al., 2021).

Recent trends in ransomware attacks indicate an increased focus on high-value targets and critical infrastructure. Attackers have been observed targeting large corporations and institutions with extensive MIS and ERP applications, exploiting their extensive networks and the critical nature of their data (Martinez & Wang, 2023). This shift underscores the need for enhanced security measures and the importance of addressing vulnerabilities in both legacy and modern systems.

4.3. Phishing and Social Engineering Threat

Phishing and social engineering attacks represent significant threats to MIS and ERP applications. These attacks exploit human vulnerabilities to gain unauthorized access, steal sensitive information, or disrupt operations. This section provides a detailed examination of these threats, including the tools, techniques, and data involved in such attacks.

Phishing attacks are deceptive attempts to obtain sensitive information by masquerading as a trustworthy entity. They typically involve fraudulent emails, websites, or messages that trick individuals into revealing credentials or other sensitive data. The primary tools used in phishing attacks include:

1. Email Phishing: This is the most common form of phishing, where attackers send emails that appear to come from legitimate sources, such as financial institutions or corporate entities. These emails often contain malicious links or attachments designed to harvest login credentials or deploy malware (Salahdine & Kaabouch, 2019).

2. Spear Phishing: Unlike generic phishing, spear phishing targets specific individuals or organizations with tailored messages. Attackers gather personal information about their targets to craft convincing emails or messages. Tools such as data mining and social media scraping are often employed to gather this information (Alaaraj & Yassin, 2024).

3. Whaling: A subtype of spear phishing, whaling targets high-profile individuals such as executives or high-ranking officials. These attacks are meticulously designed to exploit the target's position and often involve highly sophisticated tactics (Jakobsson & Myers, 2006).

Social engineering encompasses a range of manipulative techniques used to exploit human psychology and gain access to systems or information. Key techniques include:

1. Pretexting: This involves creating a fabricated scenario to obtain information from the target. For example, an attacker might pose as a technical support representative and request verification details from an employee under the guise of troubleshooting a problem (Mitnick & Simon, 2002).

2. Baiting: In baiting attacks, attackers offer something enticing to lure victims into a trap. This could be a free software download or a prize. Once the victim takes the bait, malicious software is often installed on their system (Symantec, 2018).

3. Quizzes and Surveys: Attackers may use online quizzes or surveys to collect personal information from individuals. This information can then be used in more targeted attacks or to compromise security questions and access accounts (Hadnagy, 2018).

4. Tailgating: Also known as "piggybacking," this technique involves an attacker following an authorized person into a restricted area. By exploiting the trust of individuals who hold access rights, the attacker gains physical access to secure areas or systems (Tsohou et al., 2015).

The tools used in phishing and social engineering attacks are diverse and continually evolving. Key tools include:

1. Phishing Kits: These are pre-packaged toolkits that simplify the process of creating phishing websites and emails. They often include customizable templates and scripts for generating phishing pages (Mattioli, 2020).

2. Social Engineering Tools: Tools such as social media scraping software and data mining applications help attackers gather information about targets. These tools can analyze social networks and public records to build detailed profiles of individuals or organizations (Olmstead et al., 2021).

3. Malware: Attackers frequently use malware, such as keyloggers or remote access trojans (RATs), to steal credentials or maintain access to compromised systems. This malware can be delivered via phishing emails or malicious websites (Mirza et al., 2016).

The data targeted by phishing and social engineering attacks is often sensitive and valuable. It includes:

1. Login Credentials: Usernames and passwords are prime targets, as they can provide unauthorized access to systems and data (Mohammad et al., 2015).

2. Personal Identification Information (PII): Information such as Social Security numbers, credit card details, and addresses can be used for identity theft or financial fraud (Alaaraj & Yassin, 2024).

3. Corporate Data: For attacks targeting organizations, proprietary business information, financial records, and strategic plans are often targeted for espionage or disruption (Hadnagy, 2018).

4. Access Tokens: In systems with multi-factor authentication, attackers may target access tokens or session cookies to bypass additional security measures (Symantec, 2018).

In conclusion, phishing and social engineering attacks present a considerable threat to MIS and ERP applications. By understanding the tools, techniques, and data involved, organizations can better prepare for and respond to these sophisticated threats.

4.4. Insider Threats

Insider threats represent a significant and multifaceted risk to MIS and ERP applications. These threats emanate from individuals within the organization who may misuse their access to systems and data for malicious purposes or due to negligence. The complexity of insider threats lies in their ability to bypass external security measures and exploit inherent access privileges, making them challenging to detect and mitigate.

Insider threats can be broadly categorized into malicious and non-malicious types. Malicious insiders intentionally exploit their access for personal gain or to harm the organization, while non-malicious insiders may inadvertently compromise security due to negligence or lack of awareness (Alzaabi, 2024). Both categories pose unique challenges for MIS and ERP applications, given their central role in handling sensitive business data and operational processes.

Malicious insiders may include disgruntled employees, contractors, or business partners who use their knowledge of the organization's systems to commit fraud, steal proprietary information, or sabotage operations (Subhani et al, 2021). Non-malicious threats often involve accidental data breaches or misconfigurations resulting from inadequate training or oversight (Tavani, 2016). Both types of threats can lead to significant financial losses, operational disruptions, and reputational damage.

Insiders exploit various techniques and tools to compromise MIS and ERP applications. Common methods include:

- Data Theft: Insiders may use authorized access to download or exfiltrate sensitive data. Tools such as USB drives, cloud storage services, and email are frequently employed for data transfer (Verizon, 2023).

- Privilege Escalation: Malicious insiders often exploit vulnerabilities in access control mechanisms to gain higher levels of access. Techniques such as password cracking and exploiting software vulnerabilities are commonly used (Almushiti et al, 2023).

- Social Engineering: Insiders may leverage social engineering tactics to manipulate colleagues into divulging confidential information or granting unauthorized access (Hadnagy, 2014). Phishing and pretexting are typical examples of social engineering used by insiders.

- Sabotage: Insiders may intentionally damage or alter data within MIS and ERP applications. This could involve deploying malicious software or directly modifying system configurations (Elsadig et al., 2016).

The prevalence of insider threats is highlighted by various studies and statistics. According to the 2023 Verizon Data Breach Investigations Report, 20% of data breaches involved insider threats, with 62% of these breaches resulting from malicious insiders (Verizon, 2023). The cost associated with insider threats is substantial, with the 2022 Cost of a Data Breach Report by IBM estimating the average cost of a breach caused by a malicious insider at $4.82 million (IBM, 2022). This figure underscores the financial impact of insider threats on organizations, particularly those reliant on MIS and ERP applications.

In terms of operational impact, insider threats can lead to significant disruptions. For instance, a survey by the Ponemon Institute revealed that 60% of organizations experienced system downtime as a result of insider-related incidents, impacting productivity and customer service (Ponemon Institute, 2021). Furthermore, the reputational damage resulting from insider breaches can be severe, potentially eroding customer trust and harming the organization's market position.

4.5. Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks pose a significant threat to MIS and ERP applications. These attacks are characterized by an attempt to overwhelm a target system with a flood of traffic, rendering it inaccessible to legitimate users. This section explores the intricate details of DDoS threats, including the tools and techniques employed by attackers, their impact on MIS and ERP applications, and relevant statistical data.

DDoS attacks typically utilize a range of tools and techniques to disrupt services. The most common tools include:

1. Botnets: Botnets are networks of compromised computers or devices controlled by a central entity, often referred to as the "botmaster." These botnets are used to launch coordinated attacks by directing a massive volume of traffic towards the target system. Examples of notorious botnets include Mirai and its variants, which have been responsible for high-profile attacks (Borys et al, 2022).

2. Amplification Techniques: Amplification attacks exploit vulnerabilities in network protocols to amplify the volume of traffic sent to a target. Techniques such as DNS amplification and NTP amplification are frequently used. In a DNS amplification attack, the attacker sends a small query to a DNS server with a spoofed source IP address. The server responds with a much larger response, which is then directed towards the target, amplifying the attack's impact (Cloudflare, 2013).

3. Reflection Attacks: Reflection attacks involve sending a request to a third-party server with the target's IP address as the source. The server responds to the request, and the response traffic is directed to the target. This technique leverages the server's resources to flood the target system with unsolicited traffic (Aljuhani, 2021).

The impact of DDoS attacks on MIS and ERP applications can be profound:

1. Service Disruption: The primary objective of a DDoS attack is to disrupt services, leading to downtime. For MIS and ERP applications, which are critical for business operations, such disruptions can halt business processes, leading to operational inefficiencies and financial losses (NIST, 2021).

2. Reputation Damage: Extended downtime or service interruptions can damage an organization's reputation. Clients and customers may perceive the organization as unreliable, potentially leading to a loss of business and trust (Borys, 2022).

3. Operational Costs: Addressing and mitigating the effects of a DDoS attack incurs substantial costs. Organizations may need to invest in additional resources, such as enhanced network infrastructure or DDoS protection services, to recover from the attack and prevent future incidents (NIST, 2021).

Recent statistics underscore the growing frequency and sophistication of DDoS attacks:

1. Frequency of Attacks: According to a report by Radware (2023), there was a 40% increase in the number of DDoS attacks globally between 2022 and 2023. The report highlights that DDoS attacks have become more frequent, with attackers leveraging advanced techniques to maximize their impact.

2. Attack Size: The size of DDoS attacks has also increased significantly. In 2023, the largest recorded attack reached a volume of 1.4 terabits per second (Tbps), representing a substantial escalation from previous years (Rossow, 2014).

3. Targeted Industries: DDoS attacks are not limited to any specific industry but have been particularly damaging to sectors heavily reliant on digital infrastructure, including financial services, healthcare, and e-commerce. A study by Neustar (2022) found that 60% of financial institutions reported experiencing a DDoS attack in the past year, reflecting the sector's vulnerability.

4.6. Zero-Day Exploits

Zero-day exploits represent a significant and evolving threat to MIS and ERP applications. A zero-day exploit occurs when a vulnerability in software is exploited by attackers before the vendor has released a patch to fix it. These exploits are named "zero-day" because they are used on the same day that the vulnerability becomes known, leaving no time for the developer to address the flaw (Sullivan, 2020).

Zero-day exploits are particularly dangerous due to their unpredictable nature and the time lag between the discovery of the vulnerability and the release of a fix. These exploits can be leveraged in various ways, including unauthorized access to sensitive data, disruption of services, or implantation of malware. According to a report by Symantec (2021), zero-day vulnerabilities accounted for 20% of all detected exploits in 2020, underscoring their prevalence and the need for heightened vigilance.

Attackers utilize a range of sophisticated tools and techniques to deploy zero-day exploits. One common method involves the use of automated exploit kits, which are designed to scan for and exploit vulnerabilities in software (Eshete et al, 2015). These kits are often sold on dark web forums and can be used by both skilled hackers and less experienced cybercriminals.

Additionally, advanced persistent threats (APTs) often employ zero-day exploits as part of a multi-stage attack strategy. APTs are typically well-funded and organized, using zero-day vulnerabilities to gain initial access before escalating their attacks (Mandiant, 2020). Techniques such as spear phishing or drive-by downloads are often employed to deliver zero-day exploits to target systems.

The impact of zero-day exploits on MIS and ERP applications can be profound. These applications are integral to managing critical business processes and storing sensitive information, making them attractive targets for cybercriminals. A successful zero-day attack on an ERP system could result in unauthorized access to financial data, customer records, and other proprietary information. For MIS applications, the consequences might include disruption of business operations, loss of data integrity, and compromise of confidential information (Ponemon Institute, 2022).

Data breaches resulting from zero-day exploits can have severe financial implications. A study by IBM (2023) found that the average cost of a data breach involving zero-day vulnerabilities was approximately $4.5 million, reflecting both the direct costs of remediation and the indirect costs related to reputational damage and customer loss.

In recent years, the frequency of zero-day vulnerabilities reported has been increasing. According to a report by the Zero Day Initiative (2023), there were over 100 new zero-day vulnerabilities discovered in 2022, a significant rise from previous years. This trend highlights the growing sophistication of cyber attackers and the need for robust cybersecurity measures.

Moreover, the National Vulnerability Database (NVD) reports that zero-day vulnerabilities often remain unpatched for an average of 60 days before a fix is available (NVD, 2024). This delay provides attackers with a substantial window of opportunity to exploit the vulnerabilities, emphasizing the urgency for organizations to enhance their threat detection and response capabilities.

Zero-day exploits pose a critical threat to MIS and ERP applications due to their ability to exploit unpatched vulnerabilities with no prior warning. The sophisticated tools and techniques used by attackers, combined with the significant impact on business operations and financial costs, underscore the need for organizations to remain vigilant. Understanding the nature, tools, and statistical trends associated with zero-day exploits is essential for developing effective defensive strategies.

4.7. Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) represent a sophisticated class of cyber threats characterized by their prolonged and targeted nature. Unlike conventional cyber-attacks, APTs are distinguished by their stealth, persistence, and strategic goals, making them particularly dangerous for MIS and ERP applications.

APTs are multi-phase operations that involve an extended period of reconnaissance, exploitation, and infiltration. Attackers employ a range of sophisticated techniques to gain unauthorized access to networks and systems, often with the objective of stealing sensitive information, disrupting operations, or compromising system integrity. APTs are typically carried out by well-funded and highly skilled adversaries, such as nation-states, organized crime groups, or advanced hacker collectives (Pigni et al, 2024).

APTs leverage a variety of tools and techniques to achieve their objectives. These can be categorized into several stages of the attack lifecycle:

1. Reconnaissance: This initial phase involves gathering information about the target organization to identify vulnerabilities. Tools used in reconnaissance include network scanners, social engineering techniques, and public domain information.

2. Initial Compromise: Attackers often use sophisticated phishing schemes, zero-day exploits, or advanced malware to gain initial access. Examples include spear-phishing emails with malicious attachments or links, exploiting unpatched vulnerabilities, or using custom-built exploit tools (Chen et al., 2014).

3. Establishing a Foothold: Once access is gained, attackers install malware or backdoors to maintain persistent access. This might involve using rootkits, keyloggers, or remote access Trojans (RATs) to establish control over the compromised system (Kaspersky Lab, 2018).

4. Internal Reconnaissance: Attackers perform lateral movement within the network to gather further intelligence and escalate privileges. Tools such as Mimikatz for credential harvesting or network sniffing tools may be employed (Cheswick et al., 2003).

5. Data Exfiltration: The final phase involves extracting valuable data from the target system. This can be achieved through encrypted communications, covert data channels, or by embedding data in innocuous-looking files (Symantec, 2019).

The prevalence and impact of APTs are significant. According to a 2023 report by FireEye, APT groups are responsible for 43% of all targeted cyber-attacks against enterprises (FireEye, 2023). These attacks often result in substantial financial losses, with the average cost of an

APT attack estimated at $3.86 million per incident, according to IBM's 2023 Cost of a Data Breach Report (IBM, 2023).

Furthermore, APTs are known for their high success rate in penetrating large organizations. The 2022 Verizon Data Breach Investigations Report revealed that 25% of breaches involving APTs were successful in exfiltrating data (Verizon, 2022). This statistic underscores the critical need for organizations to understand and address the advanced techniques employed by APT actors.

5. MITIGATION STRATEGIES

To effectively mitigate cyber threats targeting MIS and ERP applications, organizations must first understand the diverse and evolving threat landscape, which includes malware, ransomware, phishing, and insider threats, each requiring tailored strategies. Establishing comprehensive security policies grounded in industry best practices, such as the NIST Cybersecurity Framework and ISO 27001, forms a solid foundation for defense. Additionally, enhancing user awareness through regular training, deploying advanced technological solutions like intrusion detection systems (IDS) and artificial intelligence (AI), and implementing diligent patch management and vulnerability assessments are crucial steps. Data encryption, secure communication protocols, and regularly tested incident response plans further strengthen defenses, while continuous monitoring and improvement ensure organizations stay resilient in an ever-changing cybersecurity environment.

5.1. Understanding the Threat Landscape

To develop effective mitigation strategies against cyber threats targeting MIS and ERP applications, it is imperative first to comprehend the diverse and evolving nature of these threats. Cyber threats can vary from malware and ransomware to sophisticated phishing attacks and insider threats. Each type of threat requires tailored strategies to address its specific characteristics and potential impact on organizational operations (Sikdar, 2022).

5.2. Implementing Robust Security Policies

A fundamental component of mitigating cyber threats is the establishment and enforcement of comprehensive security policies. These policies should cover all aspects of cybersecurity, including access controls, data protection, incident response, and regular security audits. Adopting industry best practices such as those outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework can provide a solid foundation for these policies (NIST, 2020). Additionally, adhering to the guidelines provided by the International Organization for Standardization (ISO) 27001 can help ensure that security measures align with international standards (ISO, 2022).

5.3. Enhancing User Awareness and Training

Human factors play a significant role in the effectiveness of cybersecurity measures. Regular training and awareness programs for employees can help mitigate risks associated with phishing attacks, social engineering, and other human-related vulnerabilities. Programs should include simulated phishing exercises and real-time feedback to reinforce best practices and improve overall security posture (Al-Daeef et al, 2017).

5.4. Deploying Advanced Technological Solutions

Incorporating advanced technological solutions is crucial for defending against cyber threats. Tools such as IDS, IPS, and endpoint protection platforms (EPP) can provide real-time threat detection and response capabilities. Additionally, leveraging machine learning and AI can enhance the ability to identify and respond to emerging threats by analyzing vast amounts of data and identifying patterns that may indicate a potential attack (Salloum et al, 2020).

5.5. Regular Patch Management and Vulnerability Assessments

One of the most effective ways to prevent cyberattacks is through diligent patch management and vulnerability assessments. Regularly updating software and systems to address known vulnerabilities is essential for maintaining a secure environment. Organizations should implement a structured patch management process and conduct periodic vulnerability assessments to identify and remediate potential weaknesses before they can be exploited by attackers (Mohamud, 2024).

5.6. Ensuring Data Encryption and Secure Communication

Data encryption and secure communication protocols are critical for protecting sensitive information from unauthorized access and interception. Implementing strong encryption algorithms for data at rest and in transit can safeguard against data breaches and ensure that even if data is intercepted, it remains unreadable without the appropriate decryption keys (Saltzer & Schroeder, 2021). Additionally, secure communication channels, such as Virtual Private Networks (VPNs) and secure socket layer (SSL) protocols, should be employed to protect data during transmission.

5.7. Developing and Testing Incident Response Plans

An effective incident response plan is essential for minimizing the impact of a cyberattack. Organizations should develop and regularly test their incident response plans to ensure preparedness in the event of a security breach. These plans should include procedures for detecting, containing, eradicating, and recovering from incidents, as well as communication strategies for informing stakeholders and regulatory bodies (Farok & Zolkipli, 2024).

5.8. Engaging in Continuous Improvement and Monitoring

Cybersecurity is an ongoing process that requires continuous improvement and monitoring. Regular reviews of security policies, procedures, and technologies are necessary to adapt to the evolving threat landscape. Implementing a continuous monitoring strategy can help organizations detect and respond to security incidents promptly and ensure that mitigation measures remain effective over time (IBM, 2023).

6. CASE STUDIES

This section presents detailed case studies to illustrate various cyber threats faced by MIS and ERP applications. These case studies provide real-world examples of how different organizations have encountered and responded to cyber threats, offering insights into the effectiveness of various mitigation strategies.

6.1. Case Study 1: The Target Data Breach

In 2013, Target Corporation experienced one of the most significant cyberattacks in retail history, which compromised the personal and financial information of over 40 million customers (Riley, 2014). The breach originated from a third-party vendor, which had provided Target with a network connection for managing its HVAC systems. Attackers exploited vulnerabilities in the vendor's system to infiltrate Target's network.

The breach highlighted vulnerabilities in Target's ERP systems, particularly in their data protection and transaction processing modules. The attackers were able to install malware on Target's POS (Point of Sale) systems, which directly impacted the company's transaction data integrity and customer information security.

Post-breach, Target implemented several security measures, including enhanced network segmentation, improved third-party vendor management, and more robust monitoring systems (Zetter, 2014). The company also focused on strengthening its incident response protocols and investing in advanced cybersecurity technologies.

6.2. Case Study 2: The WannaCry Ransomware Attack

In May 2017, the WannaCry ransomware attack affected hundreds of thousands of computers globally, including those used in critical sectors such as healthcare and manufacturing (Askarifar et al, 2018). The ransomware exploited a vulnerability in Microsoft Windows operating systems, encrypting data and demanding ransom payments in Bitcoin.

The attack disrupted ERP systems across various industries, as it encrypted files and rendered critical business processes inoperable. Healthcare organizations, such as the UK's National Health Service (NHS), faced significant operational disruptions due to the attack, impacting their MIS applications related to patient management and clinical data.

Organizations responded to WannaCry by implementing immediate patches to fix the exploited vulnerability, enhancing their backup systems, and revising their cybersecurity policies to include regular updates and vulnerability assessments (Rashid, 2017). The incident underscored the necessity of maintaining up-to-date software and robust backup procedures.

6.3. Case Study 3: The SAP Data Breach Incident

In 2018, a data breach affecting SAP systems exposed sensitive information of several large enterprises (Syed et al, 2024). Attackers exploited vulnerabilities in SAP's enterprise software to access unencrypted data and gain unauthorized access to critical business processes.

The breach had severe implications for ERP systems, exposing confidential business data and impacting financial transactions. The compromised data included financial reports and employee records, which led to substantial reputational damage and operational disruptions for the affected companies.

In response, SAP enhanced its security features, including encryption of sensitive data and more rigorous authentication protocols. Affected organizations also invested in comprehensive security audits and improved their internal controls to prevent future breaches (Dalal & Mahjabeen, 2014).

6.4. Case Study 4: The Equifax Data Breach

In 2017, Equifax, one of the largest credit reporting agencies, suffered a data breach that exposed sensitive personal information of approximately 147 million individuals (Kenny, 2018). The breach was due to a failure to patch a known vulnerability in the Apache Struts framework used by Equifax.

The breach impacted Equifax's MIS and ERP applications by compromising critical consumer data, including Social Security numbers and credit reports. The breach exposed significant gaps in Equifax's data protection measures and incident response strategies.

Following the breach, Equifax undertook a major overhaul of its cybersecurity practices, including improving its vulnerability management program and investing in advanced threat detection systems (Zhao, 2019). The company also faced significant legal and financial repercussions, emphasizing the importance of proactive security management.

These case studies illustrate the diverse range of cyber threats that can impact MIS and ERP applications, underscoring the importance of robust security measures and proactive risk management. By analyzing these incidents, organizations can better understand the vulnerabilities in their systems and adopt more effective strategies to safeguard their critical business applications.

7. RISK MODELLING

In assessing the types of cyber threats that MIS and ERP systems face, we can develop a risk model for total risk (*R*) involving independent variables that represent the different types of cyber threats and dependent variables to indicate the impact of these threats on system integrity, operational efficiency, financial stability, and reputational risk.

Here's an analytical framework for the risk model, focusing on each variable's influence and interaction:

7.1. Independent Variables: Types of Cyber Threats

Each cyber threat serves as an independent variable, contributing uniquely to the overall cybersecurity risk faced by MIS and ERP systems. The key threats identified include:

- Malware (X_1): Includes viruses, worms, Trojans, ransomware, and spyware, each of which has a distinct mechanism of attack that impacts data integrity, system availability, and confidentiality.

- Ransomware (X_2): Specifically targets data accessibility by encrypting files and demanding a ransom, directly influencing operational continuity and financial stability.

- Phishing and Social Engineering (X_3): Manipulates human vulnerabilities to gain unauthorized access, compromising sensitive information and access controls.

- Insider Threats (X_4): Involves malicious or negligent actions from within the organization, challenging to detect due to inherent trust and access levels.

- Distributed Denial of Service (DDoS) (X_5): Overloads systems with excessive traffic, disrupting services and impacting accessibility.

- Zero-day Exploits (X_6): Targets unpatched vulnerabilities, presenting an unpredictable and sudden risk.

- AI-Specific Risks (X_7): Algorithmic bias, adversarial attacks, and data poisoning disrupt analytics and decision-making.

- Vendor Lock-in (X_8): Dependence on a single cloud provider limits flexibility and increases the cost of transition.

- Shared Technology Vulnerabilities (X_9): Multi-tenancy in cloud platforms creates exposure to side-channel attacks or resource contention.

- Service Downtime (X_{10}): Outages from cloud providers disrupt MIS and ERP availability.

- Data Sovereignty and Compliance Risks (X_{11}): Hosting data across jurisdictions introduces compliance challenges and exposure to conflicting regulations.

These variables represent the breadth of cybersecurity threats affecting MIS and ERP systems and serve as a foundation for analyzing the probability and severity of impacts.

7.2. Dependent Variables: Impact Dimensions

The model's dependent variables reflect the impact of these threats, with each threat having varying degrees of influence that demonstrate of the total risk (*R*) of the organization in the model:

- Data Integrity (Y_1): Measures the extent to which a threat compromises data accuracy, reliability, and consistency. Malware (X_1) and ransomware (X_2) threats, for example, heavily influence data integrity by corrupting or encrypting data.

- Operational Continuity (Y_2): Indicates the degree to which a threat disrupts ongoing business processes. Threats such as DDoS (X_5) and ransomware (X_2) have significant negative impacts, leading to downtime and service disruptions.

- Financial Losses (Y_3): Captures direct and indirect financial impacts, including ransom payments, remediation costs, and long-term economic effects such as insurance and regulatory fines. Malware (X_1) and ransomware (X_2) are particularly impactful here.

- Reputational Damage (Y_4): Reflects the perceived reliability and trustworthiness of an organization post-attack. Threats like DDoS (X_5) and insider threats (X_4) can damage an organization's reputation, especially if clients experience downtime or data breaches.

7.3. Coefficients and Parameters

The risk model uses coefficients to represent the weight or influence of each independent variable on the dependent variables. This can be quantified based on historical data, industry benchmarks, or expert analysis:

- β_1 to β_8: Represent the strength of the impact each cyber threat (independent variable) has on each impact dimension (dependent variable). For instance, β_2 (the coefficient for ransomware) might be relatively high for financial losses (Y_3), reflecting the significant financial burden ransomware poses.

- Interaction Terms: Certain threats may exhibit interaction effects, where the presence of one threat exacerbates the impact of another. For example, insider threats (*X_4*) could amplify the risk of malware (*X_1*) by introducing vulnerabilities from within, suggesting a combined impact on data integrity and operational continuity.

A non-linear regression equation could illustrate the relationship between cyber threats and their impacts:

$$R = \alpha + \sum_{i=1}^{8} \beta_i X_i + \sum_{i=1}^{8} \sum_{j=i+1}^{8} \gamma_{ij} X_i X_j + \sum_{k=1}^{4} \delta_k Y_k + \epsilon$$

Where:

- *Yj* represents each impact dimension (e.g., data integrity, operational continuity).
- *Xi* corresponds to each type of cyber threat.
- *βi* indicates the strength of the impact from each independent variable.
- *γkl* Interaction coefficients capturing compounded risks (e.g., shared technology vulnerabilities amplifying insider threats).
- δ_k represents the coefficient for each dependent variable Y_k, highlighting the influence of the impact dimensions on total risk.
- *α* is the model intercept.
- *ε* is the error term, capturing unmeasured factors.

7.4. Key Phases for Running of the Model

- Data Collection: Gathering data on the frequency and severity of each threat (e.g., malware, ransomware, cloud service risks) within the organization. This may involve historical incident reports, security logs, expert analysis, and industry benchmarks.
- Coefficient Estimation: Using regression techniques (e.g., multiple regression or non-linear regression, depending on the data distribution) to estimate the coefficients β_i(beta), γ_{ij}(gama), and δ_k(delta). These coefficients reflect the strength of the relationship between each cyber threat and the dependent variables (impacts).
- Model Calibration: Continuously updating the model based on emerging threats (e.g., AI-driven risks, new vulnerabilities in cloud services) and evolving security measures. Ensure that the error term ϵ\epsilonϵ reflects any unmeasured factors that may affect the risk profile.
- Risk Assessment: Calculating the total risk R for the MIS and ERP systems by inputting the values for each independent variable and using the estimated coefficients. This will provide an aggregate measure of the cyber threats faced by the organization.
- Mitigation Strategy: Using the calculated total risk R to prioritize security efforts. Threats with higher coefficients (e.g., ransomware, cloud risks) should be addressed first with targeted defenses and mitigation strategies.

Using this model, organizations can quantify the anticipated impact of each cyber threat on MIS and ERP systems, enabling a proactive approach to cybersecurity investments and controls. By understanding which threats have the most severe impact on specific business areas, security teams can prioritize defenses, allocate resources more effectively, and implement strategic measures for high-risk areas. Moreover, continuous updating of parameters (e.g., threat prevalence) ensures that the model reflects emerging cyber risks, supporting agile risk management in a dynamic cyber landscape.

The Total Risk (*R*) approach in the function offers a more holistic and dynamic risk management model for cloud-based MIS and ERP systems, integrating cyber threats, cloud service risks, and AI vulnerabilities into a unified framework. By calculating *R*, organizations can make data-driven, proactive decisions to enhance their security posture, prioritize investments, and mitigate risks more effectively in an increasingly complex and interconnected IT environment.

This analytical approach allows for a data-driven understanding of cybersecurity threats, enabling targeted strategies to mitigate the most impactful risks to MIS and ERP applications. This formula allows organizations to quantify and prioritize their cybersecurity measures based on the threat landscape and the potential impact of each threat type.

8. CONCLUSION

In today's rapidly evolving cyber threat landscape, a proactive approach to cybersecurity is not just recommended but imperative. This study highlights that the effectiveness of security measures significantly depends on anticipating and addressing potential threats before they materialize. The proposed model for mitigating risks emphasizes the need for continuous monitoring of emerging threats, the implementation of advanced security technologies, and the cultivation of a vigilant organizational culture. This involves integrating threat intelligence systems, utilizing predictive analytics to identify vulnerabilities, and adapting security protocols to address new attack vectors.

The modeling approach to the total risk (*R*) discussed in this study and model involves quantifying various cyber threats—such as malware, ransomware, phishing, insider threats, DDoS attacks, zero-day exploits, and APTs—by assessing their threat levels, potential impacts, and probabilities of occurrence. This quantitative model provides a comprehensive risk score that helps organizations prioritize and address the most significant threats to their MIS and ERP applications. By continuously updating security measures and performing thorough risk assessments, organizations can remain ahead of potential attackers, reducing their exposure to cyber threats and protecting the integrity of their critical systems.

The proposed risk modeling complies with the principles of ISO/IEC 27001. The identification, assessment, and mitigation of cyber threats directly map to the risk management practices outlined in ISO 27001. The standard's continual improvement approach also complements the need to adapt to new and evolving threats in the cyber landscape. Risk modeling also aligns well with the NIST Cybersecurity Framework. The framework's structured approach to identifying, protecting, detecting, responding, and recovering from cyber incidents is consistent with your model's emphasis on understanding, mitigating, and recovering from cyber threats. The detailed focus on specific threats, including insider threats, ransomware, and APTs, also corresponds to the risk management and incident response requirements in the NIST CSF.

Furthermore, the study underscores the crucial role of organizational culture in the effectiveness of cybersecurity practices. A security-conscious culture ensures that all employees, from top management to operational staff, understand their roles in safeguarding sensitive information. This culture is fostered through ongoing education, training programs, and clear communication channels for reporting security incidents. Leadership's commitment to cybersecurity, demonstrated through robust policies and resource allocation, is essential for reinforcing this culture and enhancing the organization's overall security posture.

Looking forward, several areas warrant further research to advance cybersecurity for MIS and ERP applications. The exploration of emerging technologies, such as AI and machine learning, could revolutionize threat detection and response. Additionally, developing advanced, industry-specific mitigation strategies and examining the balance between cybersecurity investments and organizational performance are critical for optimizing security measures. As regulatory landscapes evolve, aligning security practices with compliance requirements will also be essential for effective risk management.

In conclusion, the diverse and evolving nature of cyber threats, such as malware, ransomware, phishing, insider threats, DDoS attacks, and advanced persistent threats (APTs), poses significant risks to MIS and ERP applications. Each threat vector has unique characteristics, from malware's capacity to corrupt and exfiltrate data to ransomware's financially devastating impact through data encryption and extortion. Phishing and social engineering prey on human vulnerabilities, while insider threats exploit privileged access within organizations. DDoS attacks overwhelm systems with traffic, causing service disruptions, and APTs involve prolonged, covert intrusions with the intent to exfiltrate data over time. By quantifying the relationships between these cyber threats and their impact on critical business factors such as data integrity, financial stability, and operational continuity, organizations can employ risk modeling to develop robust cybersecurity strategies. Analyzing both independent and dependent variables, such as the frequency of attacks, types of malware, and attack sophistication levels, can guide organizations in deploying preventive measures and improving response capabilities. A comprehensive, data-driven understanding of these threats is essential for protecting MIS and ERP applications in an increasingly complex cybersecurity landscape.

DECLARATION OF THE AUTHORS

Approval of ethical committee: All procedures performed in studies comply with the ethical standards of comparable institutional and/or national research committees.

Declaration of Contribution Rate: The authors have equal contributions.

Declaration of Support and Thanksgiving: No support is taken from any institution or organization.

Declaration of Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

Adeusi, O. C., Adebayo, Y. O., Ayodele, P. A., Onikoyi, T. T., Adebayo, K. B., & Adenekan, I. O. (2024). IT standardization in cloud computing: Security challenges, benefits, and future directions. *World Journal of Advanced Research and Reviews*, *22*(05), 2050-2057.

Ahmadi, S. (2024). Zero Trust Architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports*, *26*(2), 215-228.

Ajiga, D. I., Ndubuisi, N. L., Asuzu, O. F., Owolabi, O. R., Tubokirifuruar, T. S., & Adeleye, R. A. (2024). AI-driven predictive analytics in retail: a review of emerging trends and customer engagement strategies. *International Journal of Management & Entrepreneurship Research*, *6*(2), 307-321.

Alaaraj, A., & Yassin, A. (2024). *Investigating cybersecurity response strategies: Measures to responding to successful spear phishing attack* [Dissertation]. https://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-24066

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017, July). Security awareness training: A review. In *Proceedings of the world congress on engineering* 1, pp. 5-7.

Alhalboosi, F. H. A., Mawlood, S. J., & Al-halboosi, I. A. M. (2021). Role of ERP systems in improving human resources management processes. *Review of International Geographical Education Online*, *11*(4), 1667-1681.

Aljawarneh, N., & Al-Omari, Z. (2018). The role of enterprise resource planning systems ERP in improving customer relationship management CRM: An empirical study of safeway company of Jordan. *International Journal of Business and Management*, *13*(8), 86-100.

Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. *IEEE Access*, *9*, 42236-42264.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

Almushiti, E., Zaki, R., Thamer, N., & Alshaya, R. (2023, September). An Investigation of broken access control types, vulnerabilities, protection, and security. In *International Conference on Innovation of Emerging Information and Communication Technology* (pp. 253-269). Cham: Springer Nature Switzerland.

Alquwayzani, A., Aldossri, R., & Frikha, M. (2024). Prominent security vulnerabilities in cloud computing. *International Journal of Advanced Computer Science & Applications*, *15*(2).

Alwashali, A. A. M. A., Abd Rahman, N. A., & Ismail, N. (2021, December). A survey of ransomware as a service (RaaS) and methods to mitigate the attack. In *2021 14th International Conference on Developments in eSystems Engineering (DeSE)* (pp. 92-96). IEEE.

Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, *12*, 30907-30927.

Askarifar, S., Rahman, N. A. A., & Osman, H. (2018). A review of latest wannacry ransomware: Actions and preventions. *J. Eng. Sci. Technol*, *13*, 24-33.

Badmus, O., Rajput, S. A., Arogundade, J. B., & Williams, M. (2024). AI-driven business analytics and decision making. *World Journal of Advanced Research and Reviews*, 24(01), 616–633

Borys, A., Kamruzzaman, A., Thakur, H. N., Brickley, J. C., Ali, M. L., & Thakur, K. (2022, June). An evaluation of IoT DDoS cryptojacking malware and Mirai Botnet. In *2022 IEEE World AI IoT Congress (AIIoT)* (pp. 725-729). IEEE.

Choudhuri, S. S. (2024). *AI in ERP and supply chain management*. Academic Guru Publishing House.

Cisco. (2023). *Annual cybersecurity report 2023*. Cisco Systems. https://www.cisco.com/c/en/us/about/cybersecurity.html (Accessed on 20.11.2024)

Cloudflare. (2023). *Cloudflare blog on DDoS attack vectors*. https://www.cloudflare.com/blog/

Colmenares, L. (2009). Benefits of ERP systems for accounting and financial management. In *Allied Academies International Conference. Academy of Management Information and Decision Sciences. Proceedings, 13*(1), (p. 3). Jordan Whitney Enterprises, Inc.

Dalal, A., & Mahjabeen, F. (2014). Enhancing SAP Security in Cloud Environments: Challenges and Solutions. *Revista de Inteligencia Artificial en Medicina*, *5*(1), 1-19.

Davis, E., McGuire, K., & Robson, S. (2013). Data exfiltration: The challenge of data loss prevention. *Journal of Information Security*, *4*(2), 115-127.

Elsadig, M. A., & Fadlalla, Y. A. (2016). VANETs security issues and challenges: A survey. *Indian Journal of Science and Technology*, *9*(28), 1-8.

ESET. (2024). *The State of ransomware 2024*. ESET.

Eshete, B., Alhuzali, A., Monshizadeh, M., Porras, P. A., Venkatakrishnan, V. N., & Yegneswaran, V. (2015, February). EKHunter: A Counter-offensive toolkit for exploit kit infiltration. In *NDSS*.

Farok, N. A. Z., & Zolkipli, M. F. (2024). Incident response planning and procedures. *Borneo International Journal eISSN 2636-9826*, *7*(2), 69-76.

FireEye. (2024). *Cyber threat report: trends and insights*. FireEye, Inc.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. Wiley.

Hassan, S. A., Elakhdar, B. E., Saied, W. M., & Hassan, D. G. (2024, March). Leveraging new technologies for building a comprehensive smart MIS: integrating ERP, blockchain, IoT, context-awareness, and cloud computing. In *2024 6th International Conference on Computing and Informatics (ICCI)* (pp. 459-465). IEEE.

IBM. (2022). *Cost of a Data Breach Report 2022*. IBM Security. https://www.ibm.com/security/data-breach (Accessed on 20.11.2024)

IBM. (2023). *Cost of a Data Breach Report 2023*. IBM Security. Retrieved from https://www.ibm.com/security/data-breach (Accessed on 20.11.2024)

IBM. (2023). *Cost of a data breach report 2023*. IBM Security. Retrieved from https://www.ibm.com/security/data-breach (Accessed on 20.11.2024)

ISO. (2022). *ISO/IEC 27001:2022 Information security management systems – Requirements*. International Organization for Standardization.

Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Springer.

Kaspersky. (2024). *Kaspersky security bulletin: overview of 2024 threats*. Kaspersky Lab.

Leidner, D. E., & Elam, J. J. (1993). Executive information systems: their impact on executive decision making. *Journal of Management Information Systems*, *10*(3), 139-155.

Malik, N., & Bilal, M. (2024). Natural language processing for analyzing online customer reviews: A survey, taxonomy, and open research challenges. *PeerJ Computer Science*, *10*, e2203.

Malik, A. W., Anwar, Z., & Rahman, A. U. (2022). A novel framework for studying the business impact of ransomware on connected vehicles. *IEEE Internet of Things Journal*, *10*(10), 8348-8356.

Mandiant. (2020). *APT41: The Attackers who never left*. Mandiant. Retrieved from https://www.mandiant.com/resources/apt41

Marakas, G. M. (2003). *Decision support systems in the 21st century, 134*. Upper Saddle River, NJ: Prentice Hall.

Martinez, J., & Wang, Y. (2023). Targeting critical infrastructure: The evolving ransomware landscape. *International Cybersecurity Journal*, *20*(2), 112-130.

Mattioli, M. (2020). The anatomy of phishing kits. *Journal of Cyber Security Technology*, *4*(3), 150-163.

McAfee. (2023). *McAfee labs threats report: June 2023*. McAfee LLC.

Syed, Z., Dapaah, E., Mapfaza, G., Remias, T., & Mupa, M. N. (2024, August). *Evaluating the effectiveness of cybersecurity protocols in SAP system upgrades*.

Microsoft. (2024). *Microsoft security intelligence report:* Volume 26. Microsoft Corporation.

Miller, A. (2023). Ransomware trends and mitigation strategies. *Information Security Review*, 29(1), 33-47.

Mirza, Q. K. A., Mohi-Ud-Din, G., & Awan, I. (2016, March). A cloud-based energy efficient system for enhancing the detection and prevention of modern malware. In *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)* (pp. 754-761). IEEE. A10 Networks. (2024). *The state of DDoS attacks*. https://www.a10networks.com/

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: controlling the human element of security*. Wiley.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: controlling the human element of security*. Wiley.

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*, 1-24.

Mohamud, A. J. (2024). Impact of information security policies compliance (ispc) on reducing the incidence of security breaches in organizations: Systematic Literature Review.

Nagar, G. (2024). The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies. *Valley International Journal Digital Library*, 1282-1298.

National Vulnerability Database (NVD). (2024). *Zero-Day Vulnerability Statistics*. National Institute of Standards and Technology. https://nvd.nist.gov/

Neustar. (2022). *DDoS attack trends and impact*. https://www.home.neustar (Accessed on 20.11.2024)

NIST. (2021). *Managing information security risk: Organization, mission, and information system view*. NIST Special Publication 800-39. https://csrc.nist.gov/publications/detail/sp/800-39/final

Olmstead, K., Smith, A., & Rainie, L. (2021). *Social media and privacy: An exploration of data scraping and its implications*. Pew Research Center.

Palo Alto Networks. (2023). *Unit 42 cybersecurity report 2023*. Palo Alto Networks.

Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2018). Targeting Target with a 100 million dollar data breach. *Journal of Information Technology Teaching Cases*, *8*(1), 9-23.

Ponemon Institute. (2022). *2022 Cost of a data breach study*. Ponemon Institute. https://www.ponemon.org/cost-of-a-data-breach

Rahmatian, S. (2002). Transaction processing systems. *Encyclopedia of Information Systems*, *4*, 479.

Rashid, F. (2017). *How WannaCry ransomware attacked hospitals, banks, and more*. ZDNet. https://www.zdnet.com/article/how-wannacry-ransomware-attacked-hospitals-banks-and-more/

Riley, M. (2014). *Inside Target's massive data breach*. Bloomberg Businessweek. https://www.bloomberg.com/news/articles/2014-02-26/inside-targets-massive-data-breach (Accessed on 20.11.2024)

Rossow, C. (2014). Amplification Hell: Revisiting Network Protocols for DDoS Abuse. *Network and distributed system security symposium (NDSS)*. A10 Networks. (2024). *The state of DDoS attacks*. https://www.a10networks.com/

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89.

Salloum, S. A., Alshurideh, M., Elnagar, A., & Shaalan, K. (2020, March). Machine learning and deep learning techniques for cybersecurity: a review. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 50-57). Cham: Springer International Publishing.

Saltzer, J., & Schroeder, M. D. (2021). *Principles of computer system design: An introduction*. Elsevier.

SANS Institute. (2023). *Cybersecurity awareness report*. https://www.sans.org/security-awareness-training/

Shaikh, M. R., Ullah, R., Akbar, R., Savita, K. S., & Mandala, S. (2024). Fortifying against ransomware: navigating cybersecurity risk management with a focus on ransomware insurance strategies. *International Journal of Academic Research in Business and Social Sciences*, *14*(1), 1415-1430.

Sharmeen, S., Ahmed, Y. A., Huda, S., Koçer, B. Ş., & Hassan, M. M. (2020). Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. *IEEE Access*, *8*, 24522-24534.

Sikdar, K. (2022). *Cyber threat analysis and defense strategies*. Springer.

Subhani, A., Khan, I. A., & Zubair, A. (2021). Review of insider and insider threat detection in the organizations. *Journal of Advanced Research in Social Sciences and Humanities*, *6*(4), 167-174.

Symantec. (2021). *Internet security threat report 2021*. Symantec. https://www.broadcom.com/company/newsroom/press-releases

Symantec. (2022). *Internet security threat report: 2022*. Symantec Corporation.

Symantec. (2023). *Internet security threat report 2023*. https://www.broadcom.com/company/newsroom/press-releases?filtr=2023

Tavani, H. T. (2016). *Ethics and technology: Controversies, questions, and strategies for ethical computing*. Wiley.

Thomas, T., P. Vijayaraghavan, A., Emmanuel, S., Thomas, T., P. Vijayaraghavan, A., & Emmanuel, S. (2020). Adversarial machine learning in cybersecurity. *Machine Learning Approaches in Cyber Security Analytics*, 185-200.

Trend Micro. (2023). *Trend micro annual cybersecurity report*. Trend Micro Inc.

Tsohou, A., Karyda, M., & Stergioulas, L. (2015). Social engineering and security awareness: A comprehensive overview. *Computers & Security, 54*, 69-81.

Veritas Technologies. (2024). *Data protection and backup strategies: best practices*. Veritas Technologies LLC.

Verizon. (2023). *2023 Data breach investigations report*. Verizon.

Vishwanath, A., Herley, C., & Hobson, J. (2011). *The role of email and social engineering in phishing attacks*. ACM SIGSAC Conference on Computer and Communications Security, 106-118.

Walko, J., Olney, M., & Hunt, D. (2020). The rise of SaaS ERP solutions. *Management in Healthcare*, 4(4), 340-349.

Williams, H., & Davis, K. (2023). Insider threats and mitigation techniques. *Journal of Organizational Security, 10(*1), 56-71.

Zero Day Initiative. (2023). *Annual zero-day vulnerability report*. Zero Day Initiative. https://www.zerodayinitiative.com/annual-report