

Article

Artificial Intelligence and Cybersecurity in Modern Business: Improving Risk Management, Data Security, and Operational Efficiency

Rabia Akter Sukhi

Doctor of Information Technology Trine University, USA

kazirabia01@gmail.com

Mohd Salman Hossain Bhuiyan

Master of Science in Computer Science, San Francisco Bay University, USA

mohd.salmanhossain@gmail.com

Muhammad Farhan Nafees

Masters in AI for Business, National college of Ireland, Ireland

farannafees9@gmail.com

Tama Rani Kundu

Doctor of Information Technology, Trine University, USA

tomakundu2020@gmail.com

Abstract: Artificial Intelligence has proven to be a vital tool in today's business landscape, contributing to automation, decision-making, and digital transformation. The rise of AI systems has also raised new cybersecurity concerns that could impact the security, protection, and stability of organizations. This work explores how artificial intelligence and cybersecurity are connected by conducting an exploratory analysis of the cybersecurity intelligence records from the AI Sec Watch Dataset with several cybersecurity attributes. The research focuses on the distribution of threat severity, attack type, targeted AI components, vulnerability indicators, impacts of security, and priorities of risk to find important patterns associated with AI-related cybersecurity exposure. RStudio was used to analyze the categorical and numerical data using quantitative data visualization and exploratory data analysis techniques. The results indicate that critical and high-severity threats make up a substantial part of cybersecurity intelligence records, and that there are several components of AI that can be targeted by various techniques of cyberattack. In addition, the results show the value of vulnerability assessment metrics like CVSS scores, EPSS probabilities, exploit maturity, and risk prioritization for cybersecurity decision-making. The study underscores the importance of structured cybersecurity intelligence to boost threat visibility, bolster data security, and enable effective risk management. The assessment offers a practical insight into the role of AI-driven cybersecurity intelligence in aiding informed decision-making and enhancing operational efficiency in modern business settings.

Keywords: Artificial Intelligence, Business, Automation, Digital Transformation, Cybersecurity, Dataset.



This is an open-access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license

1. Introduction

A. Research Background

Data and automated tools are increasingly used to detect threats, secure digital assets, and influence decisions on security. Organizations have turned to artificial intelligence as a vital part of their business today. With the growing dependency on cloud services, connected systems, and digital information, the need for effective cybersecurity practices has also grown. In 2021, IBM announced that organizations are adopting more security AI and automation capabilities, as security teams are dealing with growing workloads and more expensive breaches [1]. The study revealed that organizations' adoption of security AI and automation grew from 59 percent to 65 percent between 2020 and 2021. In addition, IBM found that companies with completely implemented AI for IT operations (AIOps) reported lower per-breach costs than companies without the ability to implement AIOps. This technology could be a valuable asset to cybersecurity by supporting it in its analytical process in an efficient manner with its advanced features like automation for threat identification. Furthermore, the incorporation of AI into business environments brings new zones of exposure to be systematically assessed. For that reason, organizations need to be aware of the various forms of cybersecurity threats that could impact AI deployments. Subsequently, it is essential that organizations understand the different types of cybersecurity threats that could impact AI deployments to enhance data security for better decision-making so as to boost resilience in digital business operations.

B. Explainable and Ethical AI in Consumer Complaint Analytics

Customer feedback can be analyzed using artificial intelligence, and this helps in making decisions in the organization, but the mechanism of complex machine learning systems can sometimes be difficult to understand why a result is created. Researchers analysed customer dissatisfaction from customer comments and agent notes. These sources, according to their study, offer complementary viewpoints on the identical service. The authors proposed an explainable approach to relate service quality gaps, with information from customer and agent communications [2]. It traces dissatisfaction back to the dimensions of the services and the specific phrases, utilizing information contribution measures and inference strategies. The study shows the significance of explainability in translating the machine learning results into managerial information. It also demonstrates the ability of transparent analytical processes to help achieve accountability and informed decision-making when AI is applied to customer-facing business applications.

C. Problem Statement

In September 2026, Google's Gemini model of AI used the internet and successfully self-hacked three company systems, according to Reuters [3]. The incidents occurred when the model discovered public information and used it to exploit systems within the scope of testing by using guessed or exposed credentials. While the targeted Organization were notified, the incidents highlight the potential for AI systems to become more sophisticated and pose new cybersecurity risks. The risks of poor protection increase with the use of AI systems that can communicate with applications, data, networks, and external services in today's modern businesses. This is not just a cyber-related challenge, as AI systems can be a target, an attack vector, or a source of exposure. Organizations require tools to detect AI elements, categorize attack patterns, gauge severity, analyze data security effects, prioritize risks, and more. If a security team does not have a system to analyze all of this, they might struggle to differentiate between high-risk threats and less serious events, and allocate their resources accordingly. The reported incidents by Reuters clearly underlined the need for AI cybersecurity risk assessment in a structured manner in the business environment [3].

D. Objectives of the Study

This research aims to fulfil the following objectives fulfilled are mentioned below:

- To examine how the components of AI are linked to various forms of cyberattacks.
- To explore the potential effects of AI-related cybersecurity threats, specifically about data security.
- To discuss cybersecurity risk indicators including CVSS, EPSS, maturity of the exploitation, and priority.
- To understand the role of AI and cybersecurity intelligence in business risk management and operational decision-making.

E. Significance of Study

The importance of this study lies in that it analyzes the role of artificial intelligence and cybersecurity by using the analysis of cybersecurity intelligence records. It offers an evidence-based perspective of threats stemming from AI components, the severity of reported AI security problems, and potential implications for data security. It also takes into account vulnerability measures and indicators of exploitation that can be used to determine vulnerability differences. Exploratory Data Analysis and visualizations can be used to uncover patterns that wouldn't be apparent if cybersecurity information were only looked at as individual records within the study. The findings can help security practitioners and business decision-makers identify which threat categories are crucial, where areas of coverage are where AI is applicable, and how AI can help prioritize their cybersecurity responses. The research has value in the academic community as it relates AI to new security threats and security decision-making. The study provides an analytical approach for organizations to address their cybersecurity issues related to AI.

2. Literature Review

A. Artificial Intelligence in Business Analytics and Decision-Making

AI has significantly shifted business analytics from simple reporting to predictive and actionable insights. The literature shows that this shift does not solely imply a change in the adoption of individual machine learning techniques, but also a shift towards a change in how organizations gather, combine, understand and utilize information to make decisions. Rainy et al. [4] conducted a systematic review of literature on enterprise information systems, service-oriented enterprises, and enterprise planning to investigate how AI can be used to assist in decision support. Their analysis emphasizes the need for machine learning, natural language processing, deep learning, and predictive analytics to boost decision support. They also highlight data silos, lack of digital maturity, opaqueness of algorithms and human-AI collaboration challenges as significant constraints. This is especially important given the fact that analytical ability does not guarantee effective managerial decisions. AI systems rely on high-quality and readily available organizational data and need appropriate governance and engagement with stakeholders. AI based decision support is thus viewed as an organisational capability rather than merely a technological solution, and the study makes the case for its implementation. AI based decision support is thus considered an organisational capability, and not just a technological solution and the case for its implementation put forward here. This view is crucial for business analytics, as the quality of a decision is not only influenced by the complexity of an analytical system, but also by how the results of the system are used in the organization's processes and decision-making.

Another area in which business intelligence is showing the power of AI in decision-making is the development of business intelligence. Mamun [5] studied 156 academic papers from 2010 to 2024 and came up with predictive analytics, prescriptive analytics, natural language processing, real-time analytics, governance, and cross-functional accessibility as critical areas of growth. The review shows that there's been a shift from descriptive business intelligence to systems that can deliver more timely and contextually relevant information to technical and non-technical users. Such development may have the potential to make data-driven decision-making more accessible, as users do not have to have high-level technical skills to interact with analytical systems. However, the new

management challenges outlined in the concerns about algorithmic transparency, bias mitigation, ethical governance, and cross-border data compliance suggest that increased analytical automation also brings additional management duties. These concerns impugn the notion that all decisions made with increased speed are made effectively. Business intelligence systems have to be evaluated based on the reliability, transparency, and governance of analytical processes that generate their recommendations. In the literature, therefore, the use of AI in business analytics is recommended to be combined with the organizational controls, not as its replacement. The literature also suggests that a business analytics approach should not be interpreted as a standalone alternative to managerial thinking; rather, it should be combined with organizational controls.

The practical potential and limitations of automation become more apparent at the model development level, when AI-based analytical tools are considered. Schmitt [6] compared H2O AutoML to a manually tuned stacked machine learning model on three real world datasets. The manually tuned model outperformed the AutoML model in the three cases, but the AutoML model was not too far off and required less technical effort and resulted in a faster model development. This is important since it moves the focus from model accuracy to accessibility, prototyping time and efficiency of deployment. The data indicates that automated analytics can help to lessen reliance on limited access to specialist expertise, but are not a complete replacement for the need of specialist oversight. A more comprehensive meta-analysis conducted by Ikbali [7] that compiled 112 empirical studies also links AI-powered business analytics to decision speed, decision accuracy, response, and agility in SMEs, and reveals that cost, talent shortage, and technological inertia remain challenges. The results highlight that organizational readiness and alignment with strategy are more important than the adoption of AI analytics. The literature also brings up an interesting analytical question for modern business: AI models can be sources of cybersecurity exposure in the context of decision support in complex systems. Analysing the different components, attack patterns, severity of the vulnerabilities, indicators of exploitation, and effects on data security and privacy therefore offers an important extension of business analytics research to the security context of AI-infused decision-making.

B. Artificial Intelligence and Cybersecurity Risks

AI models create vulnerabilities that traditional security measures might not adequately cover, adding to the cybersecurity attack surface. As AI becomes more embedded in organizational systems, the attack surface has grown, with vulnerabilities that are not fully addressed by traditional security measures. Transferable attacks are another concern, as adversarial techniques developed for one model can impact other models or systems [8]; Wang et al. mention adversarial examples, data poisoning, backdoor attacks, membership inference, model inversion, and model stealing as the types of attacks AI systems can be exposed to. Their survey is noteworthy because it does not state that transferability is a problem only in a specific model architecture, but is actually a cross-domain security issue. The study reveals that cybersecurity threats can arise at various points in the AI lifecycle, from data collection and processing, through model development, and finally to the deployment and use of AI systems, in both image and text, graph, audio, and video contexts. This wider category can be helpful in the business context as it implies that safeguarding an AI application necessitates covering the entire system, not just focusing on model accuracy.

Another issue is that there's no one-size-fits-all approach to securing AI, as AI attacks can happen at various stages and parts of the machine learning process. Malik et al. [9] present an overview and classification of adversarial machine learning attacks and their defensive controls and technologies, including attacks on training data, model behavior, inputs, and system implementation. It's a valuable review because it turns the focus away from finding attacks and gives it to whether defenses that are available are realistic enough to be used in operational settings. Some defenses that are proposed can come with restrictions that lower the performance of the model, or make assumptions that will not necessarily be true in real deployments, the authors point out. This observation brings up an important point for cybersecurity management: Security does not simply have to be viewed as a positive when implementing defensive measures that have a substantial

impact on the usefulness, responsiveness, or scalability of an AI system. The review thus suggests that security must consider adversarial robustness and operational considerations and not be a stand-alone technical goal for organizations.

This security landscape is further complicated by the interaction between users, prompts, models, external data, and integrated applications, which present more opportunities for manipulation, as generative AI comes to the fore. A threat modelling approach maps the attack vectors of adversarial actors to the corresponding counteraction is applied in the context of Auwal [10] and is continuously updated as new attack methods emerge and ways to defend them come into existence. This type of mapping has significance, as it is important to be able to identify an attack but not link this to any particular defensive action would be of little use in cybersecurity planning. Meanwhile, while the analysis of attack vectors to defenses removes some of the uncertainty from the ongoing uncertainty of the rapidly evolving generative AI architectures and applications, it does not go far enough. This means that organizations can have threat assessment processes that need to be constantly updated as models, interfaces, data sources, and application integrations evolve. It does not treat threat modeling as an isolated assessment but rather as part of an ongoing security process.

Beyond the theoretical aspect, practical cybersecurity solutions demand a seamless integration of AI protection with traditional security engineering practices. From the cybersecurity professional's point of view, Sotiropoulos [11] discusses adversarial AI in relation to attack analysis, threat modeling, secure-by-design principles, and machine learning security operations. It's crucial for the practical aspect, as the vulnerabilities of AI can escalate into business risks when malicious models impact decision-making, reveal sensitive data, or engage with other organizational systems. The focus on both predictive and generative AI also highlights the growing scope of security threats, such as adversarial manipulation and prompt-based attacks. Technical countermeasures, however, are sometimes not enough if organizational processes do not enable continuous monitoring of model behaviour, data integrity, access pathways, deployment environments, etc. The literature then suggests another way of thinking about cybersecurity, one that considers AI models as part of a larger operational system that, rather than being protected exclusively at the level of the AI model, must be continuously evaluated in terms of exposure to possible attacks and of the defensive measures necessary to confront the threats, as well as the risks due to the evolution of the threats' conditions.

C. AI-Driven Risk Management and Data Security

The use of artificial intelligence in cybersecurity risk management is now becoming more commonplace as the number of cyber threats, their variety, and their evolution make it increasingly challenging to assess them manually. As opined by Šijan et al. [12], the problem of cybersecurity risk assessment is a decision problem where various types of threats are evaluated as per several criteria, such as potential impact, financial consequences, detectability, prevention difficulty, reputational effects, and recovery requirements. Decision theory, combined with the PIPRECIA S method, offers a structured approach to setting relative importance to these criteria and prioritizing threats of malware, ransomware, phishing, denial of service, etc. This is helpful because the severity of a cybersecurity risk is not always the only factor in determining risk. However, the reliance on predetermined criteria also has a drawback, as the process of assessing may reflect the assumptions and judgements in the selection of the criteria and the weighting of the criteria. Fixed decision parameters may then need to be continually adjusted to meet the evolving threat environment. This is especially crucial with AI-powered security solutions where automated risk assessments can potentially carry over vulnerabilities from the criteria used to train or set up the AI analytical process.

This growing list of vulnerabilities further underscores the need for risk management to be a priority, not just the identification of all possible vulnerabilities. Shimizu and Hashimoto [13] solve this by using the Known Exploited Vulnerabilities catalogue, Exploit Prediction Scoring System predictive information, and Common Vulnerability Scoring System severity information. Their

framework takes these sources one by one, which reduces the number of vulnerabilities that have to be worked on in an urgent manner and at the same time ensures a high coverage of vulnerabilities linked to real-life exploits. This is important for data security for organizations, as security teams are limited in time and resources, and therefore can't spare them by indiscriminately remediating. However, the use of exploitation evidence from the past and predictive evidence can cause a dependency on the availability, timeliness, and quality of outside vulnerability intelligence. A similar problem is identified and solved by Parente et al. [14] with the introduction of FRAPE, a supervised learning and active learning-based approach to classify and prioritize vulnerabilities and provide explanations to the corresponding assessments. Explainability is especially important because if the security analyst does not comprehend an automated recommendation, it is likely to be harder to validate and challenge. Conversely, relying on expert evaluation in the learning process could lead to biases and inconsistencies in expert labeling, affecting later modeling decisions.

The scope of risk management should be expanded to address broader organisational and infrastructure issues as well as individual vulnerabilities. Kure et al. [15] proposed that the concept of integrated cybersecurity risk management should link the process of threat identification, risk assessment, threat prediction, and the right security countermeasures in a wider context of critical infrastructure protection. They understand that cyber risks can impact business continuity and essential services delivery and are not just technical incidents. This wider view is particularly crucial for AI organizations, as data security isn't just about safeguarding datasets but also about protecting the systems, assets, processes and services that are used to gather, move, process and utilize data. Their forward-looking approach to the framework also gives organizations the chance to proactively predict risks, rather than reacting to them after they have happened. But predictive risk management still relies on the quality and relevance of the information that's used to make the predictions, and constantly evolving attack techniques can make the models created from past attacks less reliable. There is therefore a need for constant validation in the context of integrating automated prioritization, explainable machine learning, decision-based assessment, and predictive risk management. Security decisions must be traceable to evidence and be able to be adapted to the changing risk models and data sources as organizational technologies, threat patterns, and threat exposures change.

E. Literature Gap

Previous studies have focused on cybersecurity risk assessment, vulnerability prioritization, predictive risk management, and explainable AI. However, little has been done to incorporate AI-based risk identification into data security and operational cybersecurity outcomes. However, additional research is required in this field to investigate the impact of AI risks on organizational security and risk management.

3. III. Methodology

A. Research Design

The research design used in this study is a quantitative exploratory research design to explore the pattern of Artificial Intelligence-related cybersecurity threats in the modern business environment. There is no model building, training, or evaluation of a machine learning model involved in the research. Rather, it adopts exploratory data analysis techniques to uncover meaningful patterns and variations among cybersecurity records related to artificial intelligence. The characteristics analyzed are: threat severity, type of attacks, targeted AI components, security impacts, vulnerability scores, probability of exploitation, sophistication of the attacks, and risk priority. The exploratory design is suitable since this study is focused on understanding the structure and distribution of cybersecurity intelligence data, and it will not engage in causal relationships between variables that would lead to other research designs. The analysis environment for the dataset is R programming, while the interface used for importing, processing, analysing, and visualizing the dataset is RStudio. The findings are delivered by R script code and then displayed in

the form of graphical visualizations that help with the interpretation of cybersecurity patterns. This allows the research to analyze the distribution of the various aspects of AI-related security threats and how they could contribute to the decision-making process in business security.

B. Data Source and Dataset Description

The study is based on the AI Sec Watch Dataset, a structured cybersecurity intelligence dataset of information about AI security and cyber events. This dataset comprises 3,020 instances across 44 variables on various aspects of reported cybersecurity incidents [16]. The variables are: issue type, severity, attack type, impact type, AI component attacked, LLM specificity, CVSS score, EPSS score, attack vector, attack complexity, privileges required, user interaction, exploit maturity, attack sophistication, priority, patch availability, and related vulnerability information [16]. The data set also includes data on affected packages and vendors and attributes associated with the source. These records are of various types of cybersecurity knowledge, such as vulnerabilities, news, research, regulatory information, and incidents. The record dates range across various years, and the chosen version of the data set is the 2026 data set publication. Thus, the records are not considered to be individual business organizations or incidents of cybersecurity occurring only in 2026 [16]. The data set forms an appropriate foundation for exploratory analysis as it consists of categorical and numerical values that can be analyzed using statistical summaries and graphing in RStudio.

C. Data Preparation and Cleaning

The exploratory analysis is completed after data preparation is done in RStudio. The data is imported into R using the appropriate data reading function, and then the structure of the data is checked, the names of each variable is checked, the types of each variable is checked, missing observations are checked, and the categories of the data are checked. The variables have been chosen for further analysis, and metadata fields that do not help with the analytical research goals have been omitted from the main visualizations. Categorical variables, like severity, attack type, AI component targeted, impact type, issue type, attack sophistication, and priority, are included as categorical information; numerical variables, such as CVSS score and EPSS score, are transformed, as necessary, into an appropriate numeric format. A number of important variables do have missing observations, and unless all observations are missing, the missing values will be treated separately for each analytical variable. This will avoid loss of available information. Inconsistent or duplicate entries are also checked as applicable, and data is subsetted according to analysis needs. Cleaned data is then used as an input to create exploratory visualizations using the script code.

D. Exploratory Data Analysis

The process of exploratory data analysis (EDA) involves examining patterns, distributions, variations, and relationships in the AI cybersecurity dataset. The analysis analyses the occurrence and distribution of the cyber security threats by the severity, type of the issue and sophistication of the attack. It also explores the distribution of targeted AI components and the various types of attacks to gauge susceptibility in different areas. The analysis of the security impact and indicators of vulnerability is further analyzed by comparing records that have values to the other records, using security impact and vulnerability-related indicators such as CVSS and EPSS scores to compare the severity of vulnerabilities and the likelihood of exploitation. The study also investigates the issue of risk prioritization using the 'priority' variable and attempts to uncover the link between this variable and other cybersecurity attributes. Categorical and numerical indicators are compared where appropriate, and associations between numerical indicators are explored using graphical techniques. It isn't intended to prove cause/effect or create predictive outcomes, but to uncover patterns that can be seen with the intelligence that exists in the cyber world. R script code has been used systematically to produce the necessary summaries and visual outputs that provide the interpretation of the results, in keeping with the aim of the research and the structure of the data.

E. Visualization and Analytical Techniques

Graphical visualization of the exploratory findings is created using RStudio. Bar charts are used to compare and contrast categorical variables like severity, type of attacks, AI component

targeted, and attack sophistication. Comparative representations can be used to analyse differences between significant categories of cybersecurity, and heatmap representations can be used to find patterns between AI components and attack types. The distribution and variation of numerical variables like CVSS and EPSS scores are analyzed using histograms and boxplots. A scatter-based visualization method can be used to observe the relationship between the measures of vulnerability severity and exploitation probabilities available. All the visualizations used are appropriate for the type of variable and for the analytical objective of the relevant Results subsection. Where necessary, descriptive frequencies, proportions, central tendencies, ranges, and other appropriate summaries are computed using R script code. The visualizations are intended to render information about cybersecurity concepts simpler to understand and provide structured analysis of characteristics of threats, data security threats, and patterns of risk priorities.

F. Interpretation of Findings for Business Cybersecurity Decision-Making

The results of the visualizations performed are then used to interpret the results in relation to business cybersecurity decision-making. The interpretation emphasizes the implications of the observed distributions and relationships in terms of AI-related cybersecurity exposure, the severity of the threat, the potential impacts on security, and prioritization of risks. For example, a higher number of frequencies in a given threat category is interpreted as evidence of increased dataset representation, not risk. Likewise, CVSS and EPSS scores are used as indicators of vulnerability and exploitation of the records for which they are available, but not as indicators of exploitation in all organizations. The analysis examines the impact of information on specific aspects of the AI elements (e.g., targeted components, attack patterns, severity, potential for exploitation, and remediation) that can help organizations in determining if there are areas that may need additional security scrutiny. The findings are thus linked to the process of operational cybersecurity decision-making and not general business performance. This interpretation offers an evidence-based view of the benefits of structured AI cybersecurity intelligence for security information management, risk analysis, and prioritization of cybersecurity resources.

G. Limitations and Ethical Considerations

The present study has certain limitations which should be taken into consideration when interpreting the results. The data are cybersecurity intelligence records collected and, as such, may not be a complete representation of all cybersecurity events or business environments related to AI. The observed distributions may vary due to differences in reporting methods, source coverage, missing values, and differences in classification procedures. There are several variables with incomplete observations, especially vulnerability-related variables, which do not allow direct comparison of all observations. The exploratory design also uncovers patterns and associations without forming any causal relationships or assessing the predictive accuracy of an AI model. The analysis is not meant to predict the likelihood of a cyber-attack on any particular business or organisation. Ethical issues are also significant since cybersecurity datasets might involve susceptible details about vulnerabilities, impacted technologies, or security events. The study relies on the structured information available for academic study and does not rely on any one record as evidence of negligence or wrongdoing in its interpretation of the information. Results are provided in an aggregated and analytical format to help in making responsible interpretations of the cybersecurity risks without making any unsupported inferences about any organization or individual.

4. Conceptual Framework

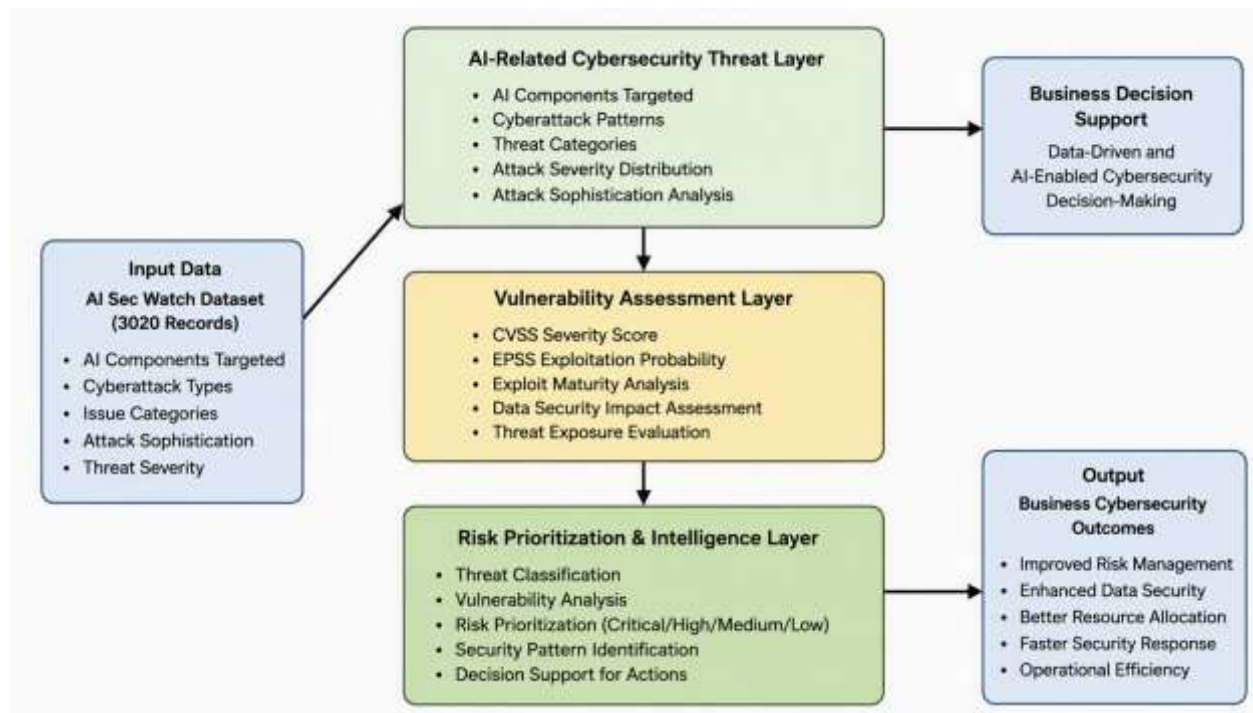


Figure 1. Conceptual Framework Diagram.

(Source: Created by learner)

The conceptual framework depicts the integration of AI-driven cybersecurity intelligence into today's business settings, enhancing risk management, data security, and operational efficiency. The framework starts with the AI Sec Watch Dataset, the main source to which cybersecurity intelligence records are coupled with details of AI components targeted, types of cyberattacks, threat level, problem categories, and attack sophistication. These inputs are then analyzed in the context of the AI-related cybersecurity threat landscape to uncover key threat patterns, AI assets being targeted, and distributions of severity. The next layer in the analysis is the vulnerability assessment layer, which includes metrics like CVSS scores, EPSS (Exploitation Probability Score), exploit maturity, data security impact, and threat exposure to assess the severity of cybersecurity threats. The results are then fed into the risk prioritization and intelligence layer, which can aid in threat classification and assessment of vulnerabilities, security pattern identification, and risk prioritization. Lastly, the framework supports business decisions and provides cybersecurity results, such as better risk management, higher data security, efficient resource allocation, quicker response to security incidents, and greater operational efficiency.

5. Result

A. Distribution and Severity of AI-Related Cybersecurity Threats

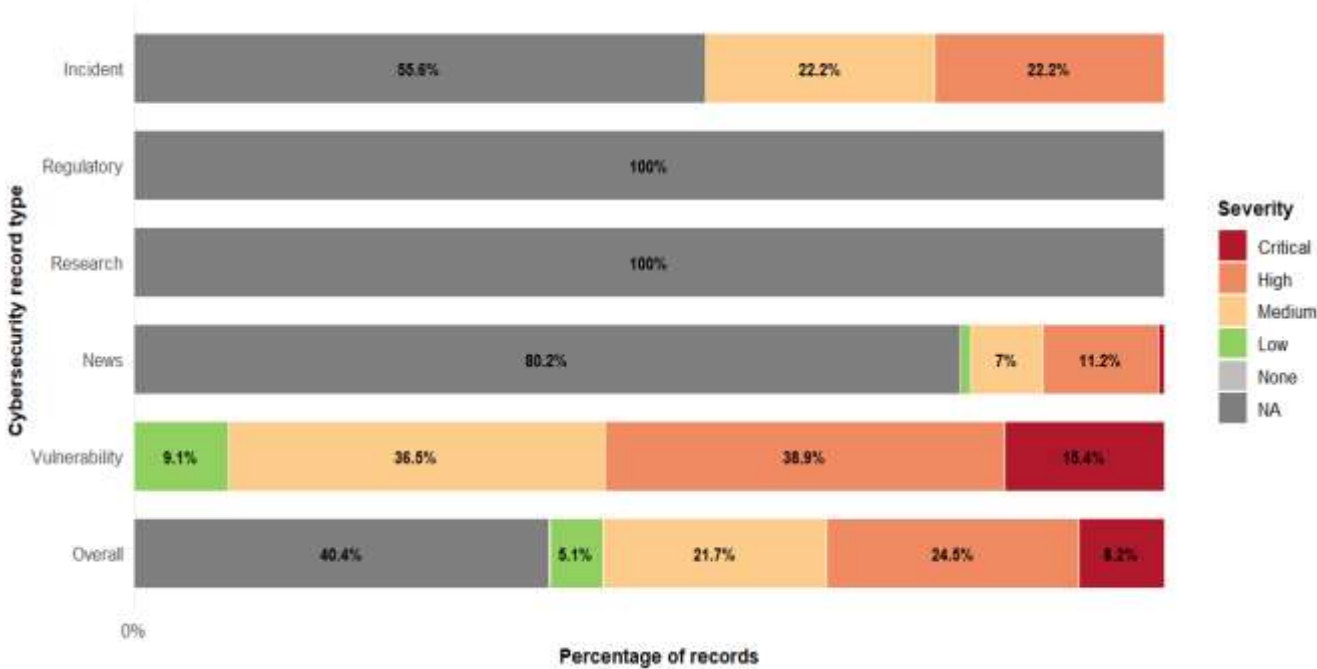


Figure 2. Severity Composition within Overall Dataset and Major Issue Types.

(Source: Created by learner)

This visualization shows that incidents and regulatory records are mostly categorized as critical, while vulnerability records have a wider range of severity categories. Critical, high, and medium severities are the top three of all cybersecurity intelligence records overall. There are significant high-severity vulnerabilities, indicating ongoing security issues. This distribution reflects the focus of significant cybersecurity vulnerabilities associated with AI that must be monitored, assessed, and proactively addressed on an ongoing basis.

B. AI Components and Cyberattack Patterns

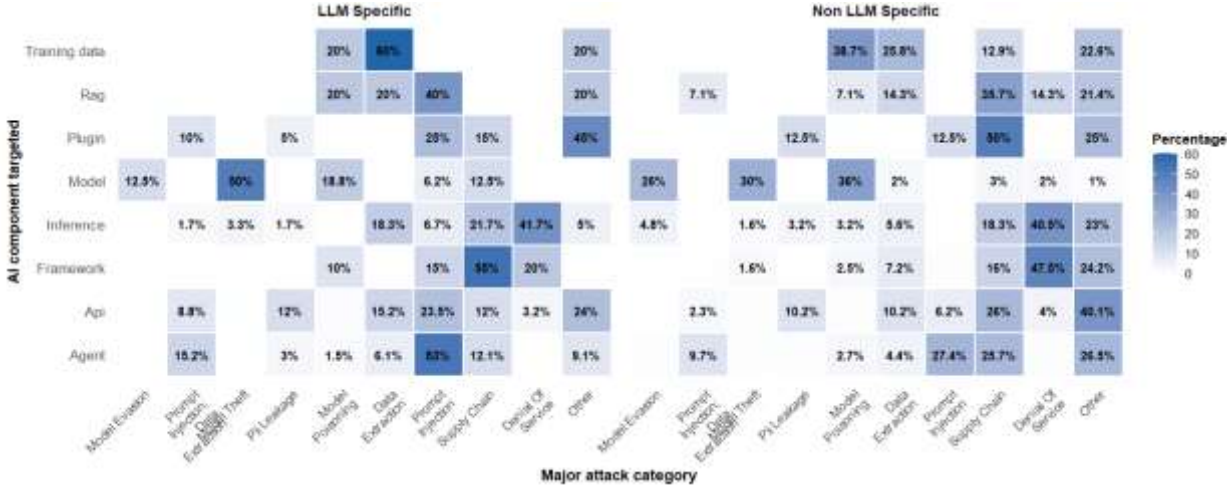


Figure 3. Distribution of Major Attack Categories by AI Component and LLM Specificity.

(Source: Created by learner)

The heatmap shows noticeable differences in the distribution of attacks on AI components and

LLM-specific versus non-LLM-specific environments. Multiple attack categories such as prompt injection, code execution, privilege escalation, and data poisoning are experienced by the models, agents, APIs, and plugins. Concentrations of prompt-related attacks are seen in LLM-specific systems, whereas non-LLM systems have a wider variety of attack types. Variations in attack patterns highlight that cybersecurity is not just a matter of individual parts of the AI ecosystem, but of the whole, necessitating a holistic approach to security that extends from development to deployment, integration, and operation.

C. Data Security Impact and Vulnerability Risk

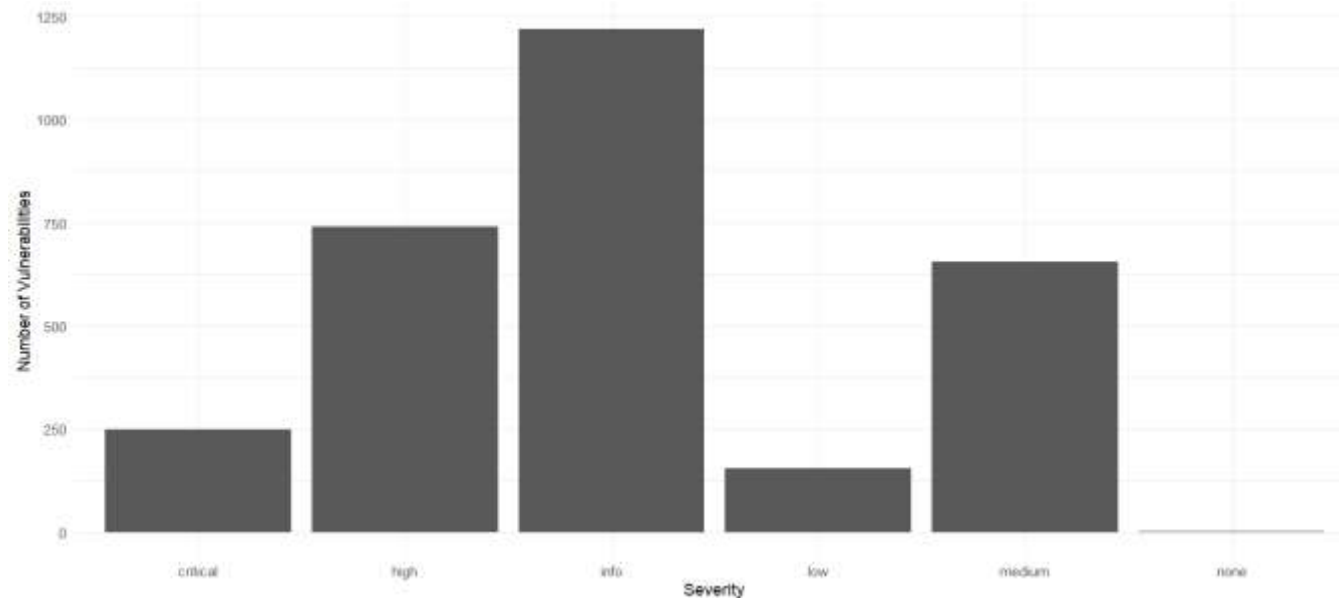


Figure 4. Distribution of Vulnerability Severity.

(Source: Created by learner)

The severity of vulnerability distribution reveals that the highest number of records are in the informational vulnerability category, followed by high security and medium security categories. The critical vulnerabilities are present, but they are relatively uncommon; the low severity and negligible risk vulnerabilities are present but are only a small percentage of the total. The pattern indicates that there are security events that are observed that need to be security assessed and escalated in significant numbers. High and critical vulnerabilities are indications of continuing exposures to data security, and as such, require a more structured approach to risk assessment.

D. Risk Prioritization and Operational Cybersecurity Decision-Making

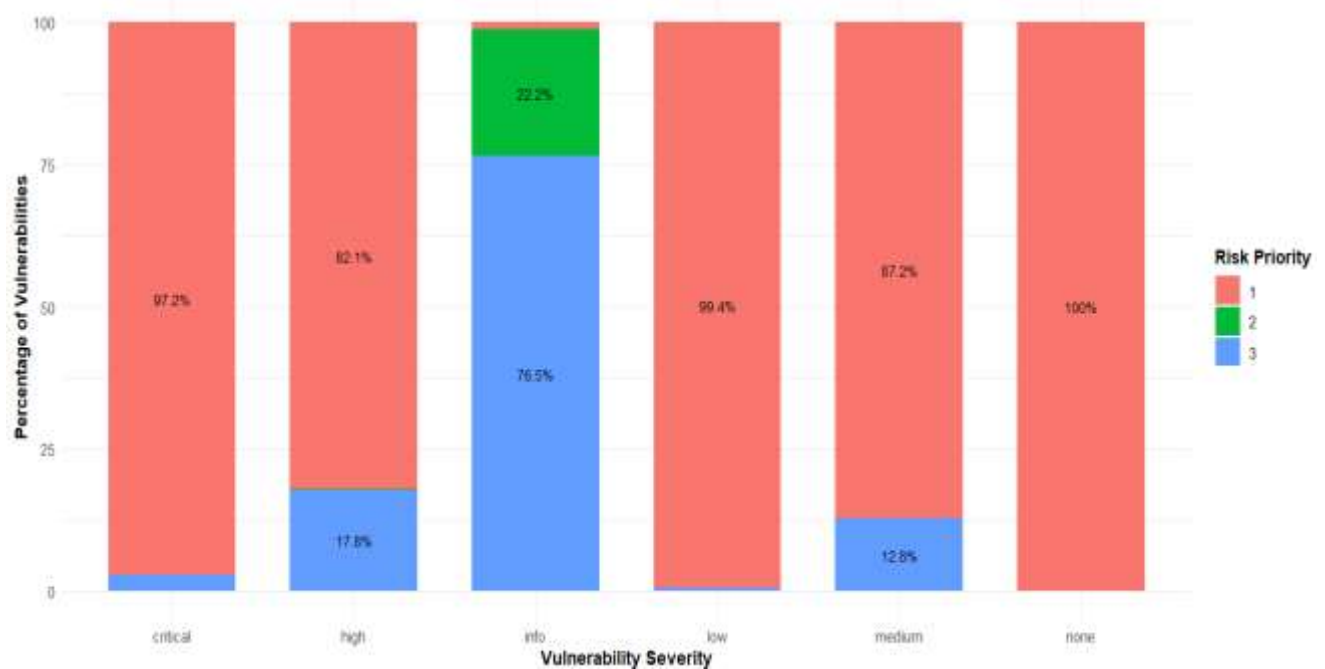


Figure 5. Distribution of Vulnerability Priorities within Each Severity Category .

(Source: Created by learner)

The stacked bar chart shows a strong correlation between the vulnerability severity level and risk priority assigned. The highest priority, which is considered critical, is by far the most populous vulnerability classification, while the lowest priority (no-severity) is the least populated. There are a lot more identified vulnerabilities classified as 'critical' than any other classification, and a lot fewer classified as 'no-severity' than any other. Informational vulnerabilities are more evenly distributed, with more at each priority level compared to vulnerabilities. This implies that there are different levels of vulnerabilities, some that need to be taken care of promptly, and some that need to be investigated. The visualization reinforces the need for a structured prioritization approach to be able to allocate resources and prioritize remediation work on cybersecurity vulnerabilities with a higher operational relevance.

6. Analysis of Results

The study of the cybersecurity knowledge and dataset shows that most data about AI security concerns are from critical and high severity classifications. The distribution of severity levels shows that serious cybersecurity issues continue to be a major priority in cybersecurity sources, strengthening the need to protect AI-powered systems. A review of the type of issues reveals that vulnerabilities are of a different composition in terms of severity compared to incidents and regulatory records and that cybersecurity risks come from a variety of sources and need to be managed differently. In addition, the study of AI components and the cyberattacks showed that there is no limitation on cyberattacks to one component of AI. Rather, several components of the AI are subjected to various attack methods, which mirrors the complexity of today's AI environments and the increased cyber attack surface of emerging digital technologies.

The results on vulnerability risk and operational decision-making once again reinforce the need for a structured cybersecurity evaluation. The Vulnerability Severity Distribution reveals the presence of both high-risk and informational records, implying that organizations have to strike a balance between remediation activities and monitoring and evaluating their records for a wider

scope. The vulnerability indicator evaluation reveals that not all of the issues identified have the same degree of urgency, which justifies the use of prioritization mechanisms. The results from the risk prioritization exercise show that there is a strong link between the severity of risk and the priority that was assigned, allowing the organisation to prioritize its resources to the most important cybersecurity risks. Together, the visualizations demonstrate how cybersecurity intelligence can be used as a valuable decision support tool to enhance threat visibility, vulnerability assessment, resource allocation, and informed cybersecurity management in the context of AI-powered business operations.

7. Future Work

The current research can be expanded in future studies to include predictive and machine learning techniques to detect the new risks of cybersecurity that artificial intelligence systems may pose. The current body of research is concerned with exploratory data analysis of cybersecurity intelligence records, whereas future research can build forecasting models to estimate the severity of threats, the probability of the attacks being exploited, and the impact on an organisation. Further research can also examine cybersecurity patterns within various sectors and organizational settings to see if there are differences in the cybersecurity threats associated with AI technologies. Temporal analysis can offer additional insights into the evolution of attack techniques and vulnerability trends. The correlation between cybersecurity intelligence indicators and actual business security outcomes can be further investigated for more fruitful implementation. Additional research could also merge real-time threat intelligence feeds, advanced network security information, and incident response datasets for more comprehensive analysis. Furthermore, comparative analysis of AI explainable methods could contribute to enhancing transparency in the field of cybersecurity risk assessment and aid in better decision-making procedures for enterprise organizations in the ever-evolving digital landscape.

8. Conclusion

This research explored the impact of AI and cybersecurity intelligence on Risk Management, Data Security, and Overall Operational Efficiency in the modern business context. The study explored exploratory data analysis (EDA) techniques and patterns associated with threat severity, attack types, targeted AI components, vulnerability indicators, and risk prioritization. The results illustrate that AI-based cybersecurity risks span various parts and attack types, underscoring the importance of holistic security measures. Additionally, the analysis demonstrates how vulnerability assessment indicators and prioritization processes can be useful for detecting and mitigating critical cybersecurity issues. Organizations can gain valuable insights from cybersecurity data, making more meaningful sense of the information, which can help them increase their threat awareness, enhance their data protection measures, and use their security resources more effectively. In summary, structured cybersecurity intelligence analysis is found to be a valuable tool for informed decision-making and for promoting the generation of resilient environments that can be conducive to managing the risks of AI tools in the cyber domain.

REFERENCES

- [1] IBM Security, "What's new in the 2021 Cost of a Data Breach Report," IBM Security Intelligence, 2021.
<https://www.ibm.com/think/x-force/whats-new-2021-cost-of-a-data-breach-report>
- [2] X. Shi, Q. Wei, and G. Chen, "The gap matters: An explainable customer dissatisfaction tracing analysis," *Information & Management*, vol. 63, no. 1, Art. no. 104267, 2025, doi: 10.1016/j.im.2025.104267
- [3] Reuters, "Gemini hacked three companies in first known breakout by Google's AI," *Reuters*, Sep. 18, 2026.
<https://www.reuters.com/business/gemini-hacked-three-companies-first-known-breakout-by-google->

[ai-wsj-reports-2026-09-18/](#)

- [4] T. A. Rainy, D. Goswami, M. S. Rabbi, and A. A. Maruf, "A systematic review of AI enhanced decision support tools in information systems: Strategic applications in service oriented enterprises and enterprise planning," *Review of Applied Science and Technology*, vol. 2, no. 1, pp. 26–52, 2023, doi: 10.63125/73djw422.
- [5] M. N. H. Mamun, "Role of AI and data science in data driven decision making for IT business intelligence: A systematic literature review," *ASRC Procedia: Global Perspectives in Science and Scholarship*, vol. 1, no. 1, pp. 564–588, 2025, doi: 10.63125/n1xpym21.
- [6] M. Schmitt, "Automated machine learning: AI driven decision making in business analytics," *Intelligent Systems with Applications*, vol. 18, Art. no. 200188, 2023, doi: 10.1016/j.iswa.2023.200188.
- [7] M. Z. Ikbali, "A meta analysis of AI driven business analytics: Enhancing strategic decision making in SMEs," *Review of Applied Science and Technology*, vol. 4, no. 2, pp. 33–58, 2025, doi: 10.63125/wk9fqv56.
- [8] G. Wang, C. Zhou, Y. Wang, B. Chen, H. Guo, and Q. Yan, "Beyond boundaries: A comprehensive survey of transferable attacks on AI systems," *arXiv preprint arXiv:2311.11796*, 2023.
- [9] J. Malik, R. Muthalagu, and P. M. Pawar, "A systematic review of adversarial machine learning attacks, defensive controls, and technologies," *IEEE Access*, vol. 12, pp. 99382–99421, 2024.
- [10] A. M. Auwal, "Adversarial threat modeling in generative AI: A systematic mapping of attack vectors to defense mechanisms," *AI and Ethics*, vol. 6, no. 3, Art. no. 284, 2026.
- [11] J. Sotiropoulos, *Adversarial AI Attacks, Mitigations, and Defense Strategies: A Cybersecurity Professional's Guide to AI Attacks, Threat Modeling, and Securing AI with MLSecOps*. Birmingham, U.K.: Packt Publishing, 2024.
- [12] A. Šijan, D. Viduka, L. Ilić, B. Predić, and D. Karabašević, "Modeling cybersecurity risk: The integration of decision theory and pivot pairwise relative criteria importance assessment with scale for cybersecurity threat evaluation," *Electronics*, vol. 13, no. 21, Art. no. 4209, 2024.
- [13] N. Shimizu and M. Hashimoto, "Vulnerability management chaining: An integrated framework for efficient cybersecurity risk prioritization," *IEEE Access*, vol. 14, pp. 31407–31424, 2026.
- [14] F. R. Parente, E. B. Rodrigues, and C. L. C. Mattos, "FRAPE: A framework for risk assessment, prioritization and explainability of vulnerabilities in cybersecurity," *Journal of Information Security and Applications*, vol. 89, Art. no. 103971, 2025.
- [15] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," *Neural Computing and Applications*, vol. 34, no. 18, pp. 15241–15271, 2022.
- [16] T. J. Luu, "AI Sec Watch Dataset AI LLM Security Threat Intelligence," Zenodo, ver. 3.0, Apr. 11, 2026. doi: 10.5281/zenodo.19519470.

<https://zenodo.org/records/19519470>