nexustek

Comprehensive AI Security Strategies to Ensure Data Integrity

How businesses can mitigate data access and control risks to enhance data governance and safeguard AI implementations.

NEXUSTEK WHITE PAPER

NexusTek Headquarters | 5889 Greenwood Plaza Blvd, Suite 201 | Greenwood Village, CO 80111 | 877.470.0401 | www.nexustek.com | info@nexustek.com

nexustek

Table of Contents

03 **EXECUTIVE SUMMARY**

04 **THE GROWING ROLE OF AI IN BUSINESS**

05 **UNDERSTANDING AI AND DATA SECURITY**

06 **THE RISKS OF AI**

A. Data Sharing Risks
B. Data Access Risks
C. AI-Specific Risks

10 **EFFECTIVE MEASURES TO SAFEGUARD YOUR AI SYSTEMS**

12 **HIRE AN EXPERIENCED IT SERVICE PROVIDER**

A. Questions to Ask Your IT Provider When Implementing AI Security Measures

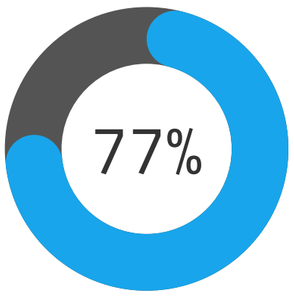
15 **NEXT STEPS WITH NEXUSTEK**

Executive Summary

As artificial intelligence (AI) continues to revolutionize industries, it brings about significant benefits but also introduces new security challenges that organizations must address. In this white paper, we will explore the critical security implications of data sharing and access when implementing AI applications in business environments, including:

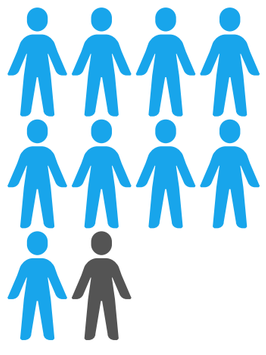
- Highlight how companies are increasingly integrating AI into their operations to gain competitive advantages and enhance efficiency.
- Provide an overview of how businesses are utilizing AI in various functions, such as customer service, cybersecurity, and digital assistants, as well as the associated security challenges.
- Focus on the risks associated with data sharing and access in AI applications, including data breaches, privacy violations, and third-party vulnerabilities.
- Detail the specific risks related to data integrity, unauthorized access, API security, and the lifecycle management of data within AI systems.
- Provide actionable steps for businesses to enhance data security in their AI implementations, including encryption, access controls, regular audits, and employee training.
- Help organizations understand the critical questions they need to ask their IT providers when implementing AI security measures, covering policies, threat modeling, data governance, and more.
- Offer specific recommendations for businesses to fortify their AI data security frameworks and ensure compliance with evolving regulations.

The Growing Role of AI in Business



77% of companies are either using or exploring the use of AI in their businesses.[12]

AI is rapidly transforming the business landscape, becoming an integral part of modern business strategies. Organizations across various industries are increasingly integrating AI to enhance operational efficiency, drive innovation, and maintain a competitive edge. In fact, 83% of companies reported that using AI in their business strategy is a top priority.[12]



9 out of 10 organizations support AI for a competitive advantage.[12]

While AI in business offers numerous advantages, the rapid adoption of AI technologies can sometimes overshadow critical concerns around data security and privacy. Many organizations have integrated AI into their business processes more quickly than they have updated their security strategies and protocols. This rapid integration has created vulnerable gaps of risk exposure, necessitating a focused approach to AI security.

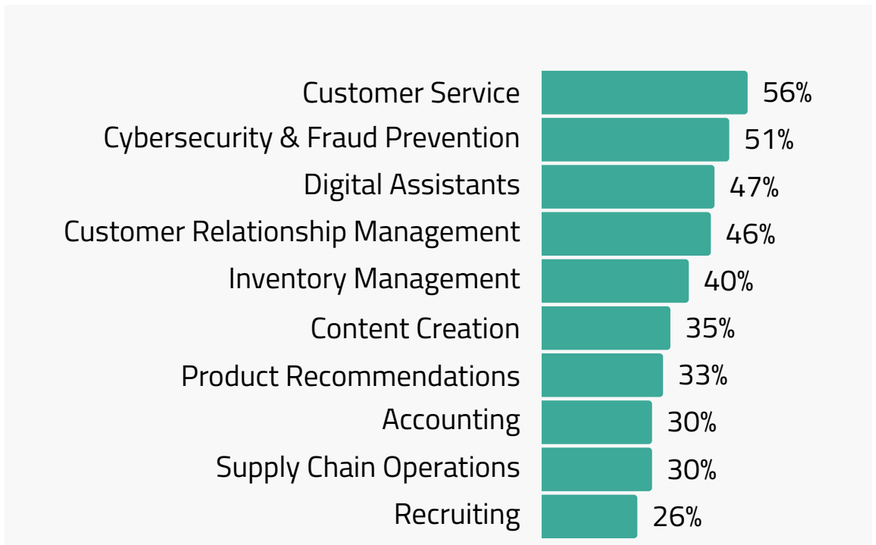
How can businesses leverage AI while ensuring robust data security and privacy?

The answer lies in a comprehensive understanding of the security implications associated with AI and implementing robust data protection measures. The purpose of this white paper is to provide an overview of the use of AI in business, the current challenges and risks, and to provide actionable strategies to mitigate risks, so businesses can utilize AI to its full potential safely and effectively.

Understanding AI and Data Security

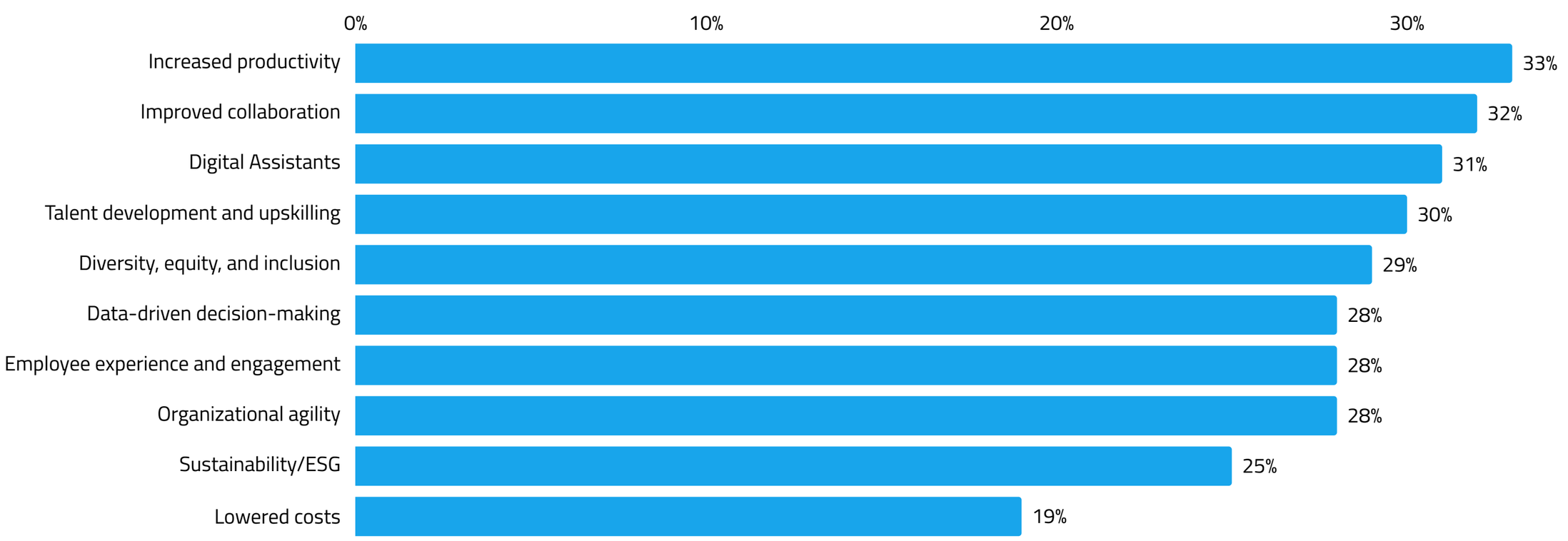
According to a recent report, **54%** of data experts say that their organization already leverages at least four AI systems or applications. Additionally, 79% report that their budget for AI systems, applications, and development has increased in the last 12 months.[6] And while the application of AI varies across industries, the most common use cases of AI in business include:

- Customer Service
- Cybersecurity
- Digital Assistants
- Customer Relationship Management (CRM)
- Inventory Management
- Content Creation
- Product Recommendations
- Accounting
- Supply Chain Operations
- Recruiting



Additionally, when business leaders were asked what they believe the biggest benefits of AI and Machine Learning (ML) integration will be. The top responses include:[7]

What do you believe the biggest benefit of AI and ML will be:[7]



However, as much as AI offers tremendous opportunities, it also poses potential risks. According to the AI Security and Governance report, 80% of data experts agree that AI is making data security more challenging.[7]

Key Security Concerns with AI - The Stats

The following are the top security threats with AI cited by nearly 700 engineering leaders, data security professionals, and governance experts:[7]

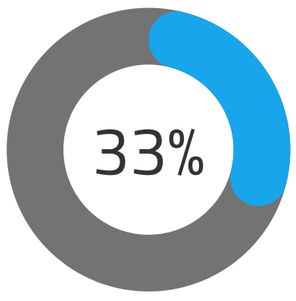
- **55%** say inadvertent exposure of sensitive information is one of the biggest threats.
- **52%** are concerned about inadvertent exposure of sensitive information via user prompts.
- **52%** worry about adversarial attacks by malicious actors via AI models.
- **57%** say that they've seen a significant increase in AI-powered attacks in the past year.

Employees at all levels are feeding data into AI models that are often not thoroughly vetted for security. According to the 2024 State of Data Security Report, 88% of data leaders reported that employees at their organizations were using AI, regardless of whether these tools were officially adopted by the company.[7] These leaders expressed widespread concern about sensitive data exposure, training data poisoning, and the unauthorized use of AI models. As AI adoption accelerates, these risks will only become more pressing. Let's now take a closer look at some of these risks to better understand the implications of integrating AI into your business model.

The Risks of AI: Navigating the Security Landscape

The primary risks associated with AI arise from the lack of effective management and proper setup by organizations. As a matter of fact, 88% of data professionals acknowledge that their employees use artificial intelligence, and 50% believe that their organization's data security strategy does not keep pace with AI advancements.[9] This data highlights the issue with the rapid adoption of AI technologies. The widespread use of AI by employees, without oversight or adequate security measures, can create substantial vulnerabilities. As organizations integrate AI into their operations, there must be a parallel enhancement in their data security strategies. Without this alignment, businesses may face increased incidents of data breaches, compromised customer information, and significant legal repercussions due to non-compliance with data protection laws.

9



33% identify a lack of visibility into data sharing and usage as their biggest security challenge.

As AI continues to integrate into various aspects of business operations, understanding and addressing these risks becomes increasingly crucial. These risks can be broadly categorized into three main areas: data sharing, data access, and AI-specific risks.

The Risks of AI: Data Sharing

Data sharing involves distributing the same data resources across multiple applications and users. This process carries inherent risks, particularly when integrating with AI systems, due to the potential for sensitive information to be exposed during transfers. Often, these vulnerabilities stem from insufficient security measures. Below, we explore specific risks associated with data sharing in AI applications:

Data Breaches

Data breaches represent a significant risk during AI implementation, characterized by unauthorized access or exposure to sensitive data. Recent statistics underscore the growing concern: the proportion of data breaches incurring costs of at least $1 million has escalated to 36% from 27% in the previous year.[13] Moreover, 77% of businesses have experienced a data breach within their AI systems over the past year, emphasizing the urgent need for robust security measures in AI applications.[13]

Data Privacy

Data privacy risks in AI implementation arise from the complex and often opaque handling of vast amounts of personal data. The potential for inadvertent exposure or misuse of this data is especially high when AI systems process and analyze it beyond typical human capacities. This can lead to scenarios where personal data is used in unexpected ways, or combined with other datasets to create detailed personal profiles, often without sufficient transparency or user consent.

- 72% of business leaders view oversharing and the exposure of sensitive information as the greatest risk associated with AI tools.[14]
- 91% of organizations recognize the importance of reassuring customers about how their data is handled.[14]
- 60% of consumers have reported losing trust in providers that use AI, driven by concerns over data privacy.[14]

These statistics underscore the crucial need for robust privacy measures and adherence to data protection laws in AI deployments.

Third-Party Risks

Third-party risks in AI applications stem from dependencies on external providers, such as commercial APIs, pre-trained models, and data, which may not meet the rigorous security standards of the primary organization. The use of these external AI tools is widespread, with 78% of organizations this year reporting that they access, buy, license, or use third-party AI solutions.[10] More concerning is the reliance on these tools, as over half (53%) of these organizations depend solely on third-party AI resources.[10] Alarmingly, 20% of these organizations do not evaluate the risks associated with these third-party AI tools at all. This oversight can introduce significant vulnerabilities, exposing the primary organization to security breaches and data mishandling if the third-party tools are compromised or misused.

Data Integrity Risks

Data integrity risks in AI applications refer to the potential for data to become corrupted or tampered with during the training and deployment of AI models. Such issues can severely undermine the reliability and accuracy of AI systems, making them less trustworthy for decision-making. Ensuring the integrity of data used in these processes is crucial, as compromised data can lead to flawed outputs, misinformed decisions, and potentially severe consequences in applications where precision is critical. Therefore, maintaining rigorous safeguards to protect data throughout the AI lifecycle is essential to preserve the trustworthiness of AI outputs.

The Risks of AI: Data Access

Data access is the on-demand ability to retrieve, modify, copy, or move data from IT systems as an authorized user. Data access risks involve the potential for unauthorized individuals to gain access to sensitive AI data due to weak access controls and authentication measures. Next, we will outline specific risks associated with data access in AI applications:

Unauthorized Access

Unauthorized access occurs when individuals exploit security gaps to access sensitive AI data without proper authorization. Such access can lead to severe consequences, including data breaches that expose confidential information, resulting in financial and reputational damage.

Access Control Weaknesses

If the access controls are not robustly set up, unauthorized users might exploit these weaknesses to access sensitive data. Common issues include insufficient authentication methods and inadequately implemented access control policies, which can inadvertently grant excessive permissions to new software components. Implementing the principle of least privilege and regularly reviewing access permissions are essential steps to mitigate these risks and ensure that only authorized entities have access to sensitive functions and data during and after any AI integration process.

API Security

APIs used by AI applications can be vulnerable to exploitation if not properly secured. APIs facilitate the interaction between AI applications and external systems, making them vulnerable to a range of security threats:

- **Authentication and Authorization Flaws:** Weak authentication and authorization mechanisms can allow unauthorized users to access sensitive AI data, enabling them to I'mpersonate legitimate users or manipulate AI operations.
- **Data Interception and Manipulation:** APIs that lack robust encryption for data transmissions are susceptible to interceptions and data breaches, posing significant risks when sensitive AI data is transmitted over networks.
- **Rate Limiting and Access Controls:** Insufficient controls can lead to API abuse, such as data scraping or denial-of-service attacks, which not only affect data integrity but also the availability of AI services.
- **Complex Configurations and Misconfigurations:** The complexity of API integrations with AI systems can lead to configuration errors, inadvertently exposing sensitive data or functionalities beyond intended limits.

Given these vulnerabilities, ensuring the security of APIs used by AI systems is essential to prevent unauthorized data access and protect the integrity of the AI operations.

The Risks of AI: AI-Specific

Compliance Violations

AI systems must comply with regulatory requirements to avoid legal penalties. Failure to adhere to data protection laws and industry standards can result in significant fines and damage to an organization's reputation.

Evasion Attacks

Evasion attacks involve designing inputs that evade AI defenses, resulting in incorrect outcomes or bypassing security measures altogether. These deceptively legitimate inputs allow attackers to manipulate results without triggering alerts, significantly compromising the AI system's reliability. Examples include:

- **Misclassification:** Deliberately crafted inputs cause the AI to misclassify sensitive data, allowing malicious activities to go undetected.
- **Security Bypass:** Inputs designed to look benign trick the AI into ignoring or underestimating threats, enabling attackers to infiltrate systems without alerting security protocols.

Model Extraction Attacks

These attacks entail the unauthorized copying or theft of trained AI models. By replicating an AI's functionality, attackers can commit intellectual property theft and misuse the capabilities of the AI, potentially leading to significant security and operational challenges.

AI-Powered Malware

AI can lower the cost and increase the effectiveness of malware generation, making it easier for attackers to develop sophisticated malware. This can lead to:

- Disruptions of services
- Hijacking of resources
- Exploitation of AI platforms

Training Data Manipulation

Injecting malicious data into training datasets, or model poisoning, can alter AI model behavior, leading to biased or inaccurate outputs. This manipulation undermines the model's integrity and reliability, affecting its overall performance and decision-making capabilities.

Understanding the various risks associated with AI allows you to take the first step toward protecting your data and preventing potential security incidents.

Effective Measures to Safeguard Your AI Systems

The implementation of mitigation strategies permits organizations to proactively address and navigate these risks, protecting their data, maintaining compliance with regulations, and ensuring the reliability and safety of their AI systems. In this section, we'll present actionable steps to harden your enterprise against data breaches, privacy breaches, and other AI-specific threats.

"Despite the evident risks, only 38% of organizations are working to mitigate risks associated with AI, McKinsey found."[15]

By following these best practices, you can reduce your risk exposure and establish a stronger security infrastructure to underpin your AI efforts.

Data Encryption

Data encryption is a security measure that involves transforming readable data into a coded form that can only be accessed and deciphered by those who have the appropriate decryption key. This process ensures that data remains confidential, whether it is being transmitted between locations (in transit) or stored (at rest).

Implementing end-to-end encryption is highly recommended for all data transfers and storage. This method ensures that sensitive information is protected throughout its lifecycle by encrypting data at multiple levels: within applications, databases, and during communication over networks using secure protocols like TLS/SSL. By doing so, encryption provides a robust defense against unauthorized access, safeguarding the information even if it is intercepted.

Access Controls

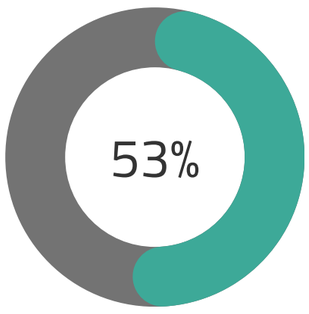
Access control involves setting up policies and technical measures to verify who can view and use sensitive AI data and systems. This process, known as identity and access management, includes mechanisms like authentication (confirming a user's identity) and authorization (granting the right to access specific resources).[16]

A significant portion of organizations, about 61%, have adopted purpose-based access controls. This strategy involves assigning specific permissions based on the user's role and responsibilities within the organization. By doing so, each individual has access only to the data and systems needed to perform their job functions, effectively preventing unauthorized use of AI models. This targeted approach helps maintain security and operational efficiency by ensuring that access is appropriately managed and restricted according to each user's requirements.

Policy Development

Policy development is crucial for ensuring that AI-specific security requirements are clearly defined and implemented. This involves reviewing and updating existing policies and procedures to address the unique challenges posed by AI technologies. Establishing clear roles and responsibilities is essential to effectively oversee AI operations and the adherence to these security guidelines.

Designating specific roles for AI oversight is a strategic move to enhance accountability and ensure comprehensive coverage of all security aspects related to AI. These roles are responsible for setting up data handling protocols, continuously monitoring AI system performance, and swiftly responding to security incidents. Such structured governance helps maintain a secure and efficient operational environment for AI applications.



53% of organizations use public AI tools without an Acceptable Use Policy.[14]

Employee Training

Currently, only 46% of organizations offer AI-specific training to their employees, highlighting a significant gap in education on AI security practices.[14] To address this, regular security awareness campaigns and training sessions are essential. These initiatives help keep employees updated on the latest threats and best practices, ensuring they have the necessary knowledge to protect AI systems effectively.

Additionally, fostering a culture of security awareness within organizations is crucial for safeguarding AI systems against potential risks. By continuously educating and engaging all stakeholders about security, organizations can ensure a vigilant and informed workforce, equipped to handle security challenges.

Threat Modeling

Threat modeling is an essential exercise for identifying and assessing potential security threats to AI systems. This process involves a systematic evaluation of vulnerabilities within the system, allowing organizations to devise effective strategies to mitigate these risks. By understanding potential attack scenarios, threat modeling provides insights into how an attacker might exploit system weaknesses. This knowledge is crucial for preparing and implementing defenses that protect AI systems from malicious actions. Through this proactive approach, organizations can enhance their security posture and ensure the integrity of their AI operations.

Data Governance

Implementing effective data governance practices ensures that data is properly classified, protected, and managed. Recent surveys indicate that 83% of IT and engineering leaders have revised their internal privacy and governance guidelines to meet the evolving challenges presented by AI.[16]

Proper data governance involves establishing clear policies for how data is handled, ensuring that these practices comply with relevant regulations, and maintaining the integrity of data throughout its lifecycle. This comprehensive approach ensures that data is used responsibly and securely, supporting the trustworthiness and effectiveness of AI systems while safeguarding sensitive information.

End-Point Security

Implementing endpoint security solutions is crucial for protecting AI systems from misuse and abuse. This form of security is vital for the early detection of any signs of compromise, allowing organizations to intervene promptly and effectively. Additionally, maintaining and regularly updating endpoint security measures ensures that they can adapt to evolving threats, safeguarding sensitive data against the latest vulnerabilities. Strong endpoint security not only preserves the integrity of AI systems but also supports a secure operational environment, crucial for the reliable functioning of these technologies.

Hire an Experienced IT Service Provider

Partnering with an experienced IT service provider can significantly enhance your organization's management and security of AI systems. An IT provider with specialized expertise in AI and cybersecurity can not only implement robust security measures and conduct regular assessments but also provide ongoing support to ensure your AI applications are secure and compliant with industry standards.

Additionally, outsourcing AI management to an IT provider offers several other benefits:

Cost Efficiency:

Outsourcing can be more cost-effective compared to maintaining an in-house team, especially for specialized tasks. It eliminates the overhead associated with training, salaries, and benefits for full-time staff.

Scalability:

As your AI needs grow, an IT provider can help scale your AI systems efficiently without the need for substantial in-house investment in hardware and expertise.

Focus on Core Business:

By delegating AI management to an expert provider, your organization can focus more on its core competencies and strategic initiatives. This allows your internal IT department to prioritize innovation and growth, rather than managing AI security and compliance.

Risk Management:

IT providers are experienced in identifying and mitigating risks, ensuring that AI applications run smoothly and securely, which in turn reduces the potential for costly disruptions.

Access to Specialized Knowledge:

IT providers possess deep insights and up-to-date knowledge in AI technologies and cybersecurity, which can be costly and time-consuming for organizations to develop internally.

Questions to Ask Your IT Provider When Implementing AI Security Measures:

Policy and Compliance Readiness:

Do we have the right policies, standards, and procedures in place to tackle AI-related security and privacy risks?

Asking about AI-specific policies and procedures is foundational to safeguarding your systems against emerging threats. Comprehensive policies should be robust, regularly updated, and specifically designed to address the unique challenges presented by AI technologies.

Do we need new policies, standards, and procedures to cover any gaps in the existing practices or emerging domains?

As AI technology evolves, so does the landscape of potential risks. It's essential to assess whether current practices are sufficient or if new policies are needed to bridge any gaps. An ideal provider continuously evolves their policies to adapt to new challenges.

Threat Modeling and Risk Assessment:

Have we conducted threat modeling exercises to identify potential security threats to AI systems and assess their impact?

Understanding potential security threats through threat modeling is an integral part of developing a robust AI security strategy. Look for detailed risk assessments that not only pinpoint vulnerabilities but also outline actionable steps to mitigate these risks

What are the criticality, connections, boundaries, data characteristics, threats, impacts, and mitigations identified in our threat modeling?

This question helps you gauge the depth and comprehensiveness of the threat modeling process. Effective threat modeling should cover a wide range of elements from data flow and storage to user access and beyond.

Data Governance and Integrity:

Do we have roles and responsibilities established for data governance?

Clear roles and responsibilities are essential for effective data governance. This ensures accountability and helps maintain the integrity and security of data throughout its lifecycle.

Are we performing regular data quality assessments and validations?

Regular data quality checks are critical for ensuring that the data powering AI systems is accurate and reliable. This forms the backbone of effective AI operations and decision-making processes.

Are our identity and access management policies in place to prevent unauthorized data modifications?

Strong identity and access management policies are crucial to protect sensitive data from unauthorized access and modifications, safeguarding your AI systems from potential breaches.

Do we have acceptable data use policies defined?

Establishing clear data use policies is vital for regulatory compliance and ethical usage of data, particularly in sectors where data sensitivity is high.

Comprehensive AI Security Strategies to Ensure Data Integrity

Access Control and Monitoring:

Who should have access to what AI systems, data, or functionality?

Limiting access to sensitive AI systems and data is a key security measure. Ensuring that access rights are clearly defined and strictly enforced minimizes the risk of data breaches.

How and when should access be re-evaluated, and by whom?

Regular re-evaluation of access controls is necessary to keep up with changes in personnel and roles, helping to maintain a secure and compliant IT environment.

What type of logging, reporting, and alerts should be in place?

Effective logging and alerting mechanisms are crucial for detecting and responding to incidents promptly, thereby reducing the potential impact of security breaches.

What access controls do we need, especially related to the data annotation process?

Data annotation involves significant access to sensitive data; thus, it requires stringent access controls to prevent unauthorized use and ensure data integrity.

Data Protection Techniques:

Are we using encryption to protect the confidentiality and integrity of AI training data, source code, and models?

Encryption is a fundamental security measure for protecting the confidentiality and integrity of critical data and intellectual property, including AI training datasets and models.

Endpoint Security and Misuse Detection:

Have we implemented end-point security solutions to detect early signs of AI misuse and abuse?

Endpoint security solutions are essential for detecting and mitigating the misuse of AI applications, providing an early warning system against potential abuses.

Infrastructure Security and Maintenance:

Are we regularly applying software updates and conducting periodic assessments of AI infrastructure components?

Regular updates and assessments ensure that AI infrastructure is protected against known vulnerabilities and is performing optimally.

Are we conducting regular penetration tests on AI solutions and functionality?

Penetration testing is critical for identifying vulnerabilities in AI systems before they can be exploited, helping to strengthen the overall security posture.

Security Training and Awareness:

Are we providing security training specific to the roles and responsibilities of executives, developers, system engineers, users, and others?

Tailored security training helps ensure that all personnel are aware of and can effectively address the security challenges specific to their roles within AI implementations.

Are we regularly updating security training materials to keep pace with the rapidly evolving threat landscape?

Continuously updated training materials are necessary to keep staff informed of the latest threats and best practices, helping to maintain a proactive stance against potential security issues.

Partner with NexusTek

Implementing AI security measures is crucial for safeguarding your organization's valuable data and systems. NexusTek, a leading provider of modern IT services, specializes in maximizing business outcomes for businesses. They offer comprehensive, secure, scalable, and cost-effective solutions designed to ensure measurable results and significant impact at every stage of a company's lifecycle. By partnering with NexusTek, you can leverage our extensive experience and customer-focused approach to enhance your security infrastructure. NexusTek's commitment to delivering comprehensive IT solutions ensures that your AI implementations are robustly protected against the evolving landscape of cyber threats.

To start strengthening your AI security posture, evaluate your current security measures and identify any potential gaps. Consider how NexusTek's services, including our expertise in cybersecurity and end-user services, can integrate with your existing systems to provide a seamless security enhancement. The next step is to reach out to NexusTek for a detailed consultation and customized security plan tailored to your specific needs.

Contact NexusTek

About NexusTek

For over 28 years, NexusTek has established itself as a leader in comprehensive IT services, boasting a 98% customer satisfaction rating and a diverse portfolio that includes AI risk management, cloud services, and cybersecurity. We are committed to delivering exceptional value and outcomes, designing each solution to maximize business performance, reduce costs, and drive revenue. Supported by a robust team of over 200 skilled IT engineers and 24/7/365 customer support, NexusTek ensures reliable and uninterrupted service. Our approach not only meets but often exceeds customer expectations, making us a trusted partner for businesses looking to enhance operational efficiency and growth.

References

1. Fatemi, F. (2019, May 29). 3 Ways Artificial Intelligence Is Transforming Business Operations. Forbes. Retrieved from https://www.forbes.com/sites/falonfatemi/2019/05/29/3-ways-artificial-intelligence-is-transforming-business-operations/?sh=5634fedc6036
2. Statista. Artificial Intelligence (AI) in Labor and Productivity. Retrieved from https://www.statista.com/topics/11516/artificial-intelligence-ai-in-labor-and-productivity/#topicOverview
3. Gartner. (2023, October 3). Gartner Poll Finds 55 Percent of Organizations Are in Piloting or Production Mode with Generative AI. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2023-10-03-gartner-poll-finds-55-percent-of-organizations-are-in-piloting-or-production-mode-with-generative-ai
4. MITRE. Public Trust in AI Technology Declines Amid Release of Consumer AI Tools. Retrieved from https://www.mitre.org/news-insights/news-release/public-trust-ai-technology-declines-amid-release-consumer-ai-tools
5. Forbes Advisor. AI Statistics. Retrieved from https://www.forbes.com/advisor/business/ai-statistics/
6. Immuta. The AI Security Governance Report: Introduction. Retrieved from https://www.immuta.com/resources/the-ai-security-governance-report-introduction/
7. Immuta. 2024 State of Data Security Report. Retrieved from https://www.immuta.com/2024-state-of-data-security-report/
8. AvePoint. (2024). AI and Information Management Report. Retrieved from https://www.avepoint.com/ebooks/ai-and-information-management-report-2024
9. PwC. Global Digital Trust Insights. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html
10. Boston Consulting Group. Building Robust RAI Programs as Third Party AI Tools Proliferate. Retrieved from https://web-assets.bcg.com/1b/18/c684f0174e088e068efc4c62c942/building-robust-rai-programs-as-third-party-ai-tools-proliferate.pdf
11. LinkedIn. How to Address Third Party AI Risk: A Guide for Business. Retrieved from https://www.linkedin.com/pulse/how-address-third-party-ai-risk-guide-business-funso-t9x9e/
12. Exploding Topics. AI Adoption in Businesses. Retrieved from https://www.nu.edu/blog/ai-statistics-trends/#:~:text=AI%20Adoption%20in%20Businesses,priority%20in%20their%20business%20plans.
13. Tech.co. Study: Business AI Security Breaches. Retrieved from https://tech.co/news/study-business-ai-security-breaches
14. SecurityInfoWatch. Data Security Risks Associated with AI Implementation. Retrieved from https://www.securityinfowatch.com/cybersecurity/article/55042639/data-security-risks-associated-with-ai-implementation
15. McKinsey & Company. Cybersecurity in the Age of Generative AI. Retrieved from https://www.mckinsey.com/featured-insights/themes/cybersecurity-in-the-age-of-generative-ai
16. PR Newswire. AI Security & Governance Survey Finds That AI Is a Double-Edged Sword as Organizations Weigh the Risks and Rewards. Retrieved from https://www.prnewswire.com/news-releases/ai-security--governance-survey-finds-that-ai-is-a-double-edged-sword-as-organizations-weigh-the-risks-and-rewards-302130926.html
17. AvePoint. Enhancing AI Training Programs for Organizational Success. Retrieved from https://www.avepoint.com/blog/manage/enhancing-ai-training-programs-for-organizational-success#:~:text=However%2C%20AvePoint's%20AI%20%26%20Information%20Management,gap%20is%20real%20and%20growing.