Managing AI Security Risks

AI Security Strategic Priorities

Executive Summary

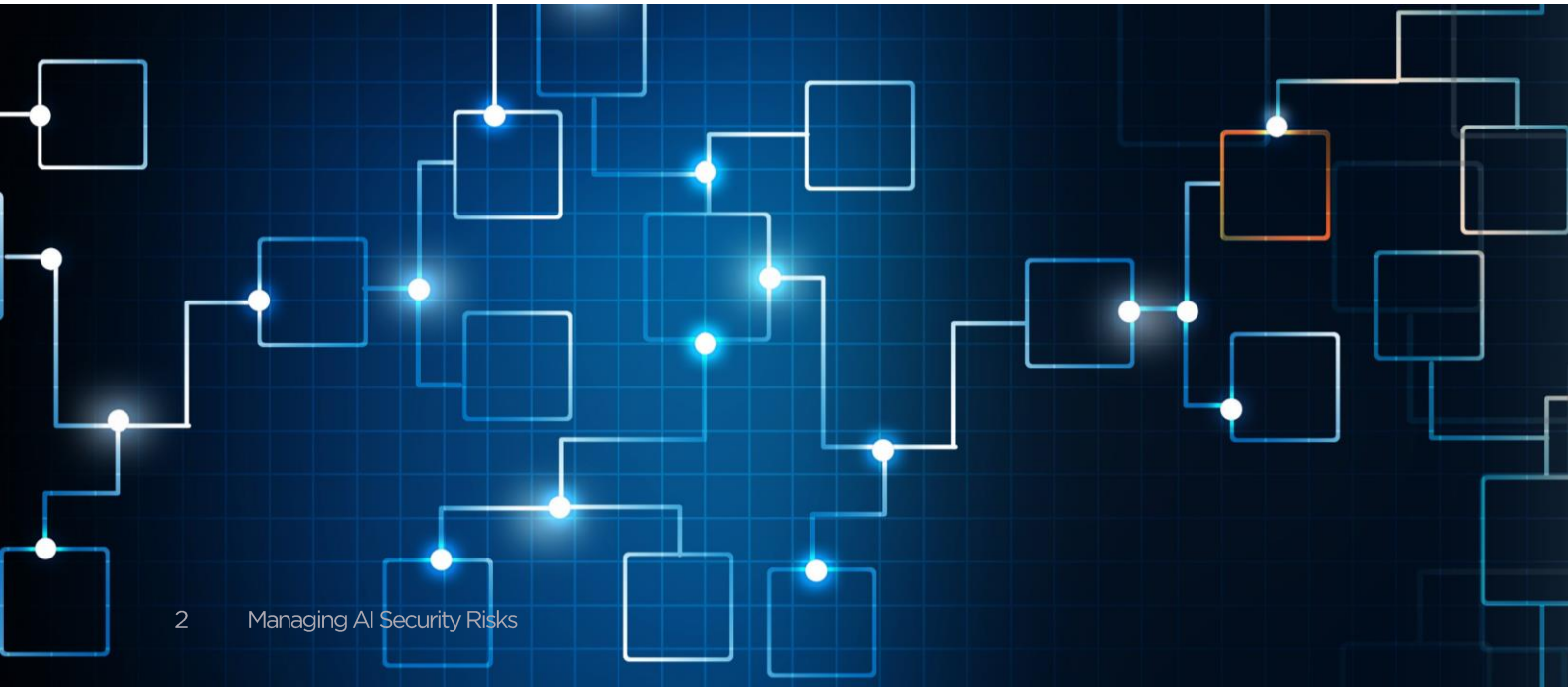
In today's rapidly evolving digital landscape, artificial intelligence (AI) has become a critical driver of innovation and operational efficiency. However, the deployment of AI technologies across organizations also presents significant security challenges. The increased complexity of AI systems, coupled with their expansive reach across the enterprise, has created new vulnerabilities that extend beyond traditional cybersecurity concerns and requires a broader aperture to manage. According to research, AI-enhanced malicious attacks, including AI-assisted misinformation have ranked as the top emerging risks for 2024[1]. As the accessibility and sophistication of AI tools increase, so does the potential for more devastating attacks. This introduces not only cybersecurity threats, but also security challenges related to model safety, data protection, and privacy, making it harder for organizations to respond effectively[2].

A recent Deloitte study further reveals that three of the top four barriers to the successful development and deployment of Generative AI (Gen AI) tools and applications are linked to security challenges. These include regulatory compliance (cited by 36% of respondents), difficulty managing risks (30% of respondents), and the lack of a governance model (29% of respondents)[3]. This is largely due

to the legal uncertainties surrounding AI adoption, including evolving privacy regulations such as General Data Protection Regulation (GDPR), the European Union AI Act (EU AI Act), and the California Consumer Privacy Act (CCPA), vertical specific risks (higher scrutiny and complexity in industries like healthcare and financial services), as well as rising consumer expectations for transparent and fair AI systems.

To be truly secure, organizations must not only protect themselves from external cyber threats but also address internal risks, business vulnerabilities, and legal and reputational risks. A secure organization is one that defends itself from all these risk vectors—whether cyber, business, or regulatory in nature—ensuring robust defenses across the enterprise. While AI introduces security risks, the business benefits—such as operational efficiency, automation, and innovation—far outweigh these challenges when the risks are managed intentionally. By adopting AI, organizations can gain a competitive edge with data-driven insights and streamlined processes. The risks can be effectively managed through a robust AI Security Risk Framework that ensures data protection, model safety, and compliance. With the right security measures, the value of AI adoption becomes a strategic necessity. This requires building organizational capacity for proactive risk management and establishing robust security protocols that align with both regulatory requirements and emerging threats.

This paper outlines the security risks and vulnerabilities inherent in organizations AI systems, along with a comprehensive AI Risk Framework. It offers suggestions for organizations



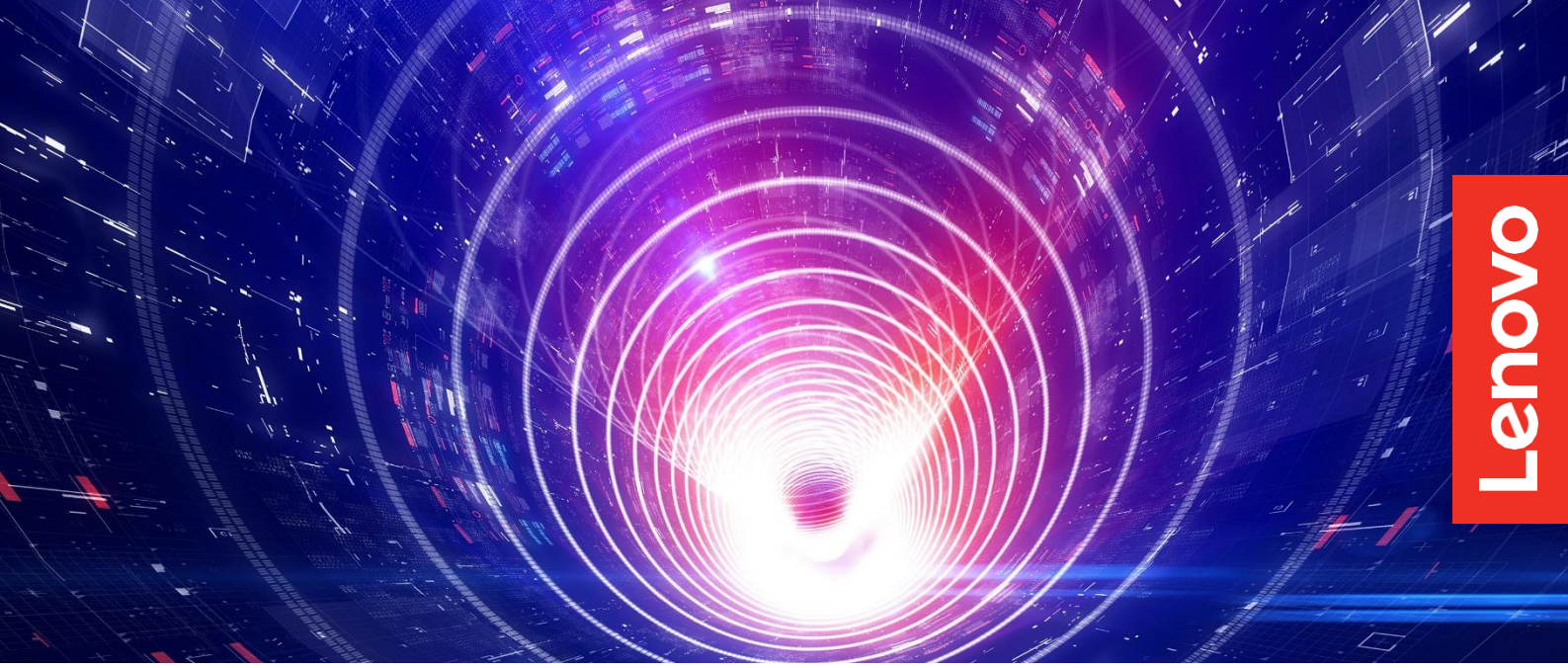
across process and technology capabilities to mitigate these challenges, strategic priorities for leadership, and actionable steps for IT Decision Makers (ITDMs) and Chief Information Security Officers (CISOs) along with other executives to more resiliently navigate AI's complex security landscape.

Strategic Priorities for Leadership When Building an AI Security Foundation

In the third global annual survey of Chief Information Officers (CIOs) by Lenovo, 51% of CIOs said that cybersecurity remains a top priority for IT, and 65% said they find it challenging to address data privacy and security[11]. As organizations strive to secure their AI systems, leadership—particularly ITDMs and CISOs—must prioritize organization-wide strategies to effectively implement the AI Security Risk Framework.

"51% of CIOs said that cybersecurity remains a top priority"

1. **Implement Clear Governance Frameworks:** Leaders must prioritize robust governance frameworks that clearly define roles, responsibilities, and accountability for AI security. This includes establishing policies and standards that align with regulatory requirements and organizational objectives. AI governance should be embedded in the broader enterprise risk management strategy, ensuring that AI security risks are managed alongside other organizational risks. Hiring a Chief Artificial Intelligence Officer (CAIO) can accelerate the implementation of governance frameworks and enable more effective oversight.



2. **Build Continuous Monitoring:** Implementing DevSecOps practices ensures security is embedded at each stage of the AI development lifecycle, integrating continuous security checks into CI/CD pipelines. This proactive approach, combined with advanced monitoring tools, provides real-time visibility into AI operations, detecting and mitigating threats swiftly. Continuous monitoring, combined with feedback loops and threat intelligence, allows teams to refine security measures, facilitating an agile response to evolving risks.

3. **Automate Organizational Defenses:** Automation enhances the efficiency and effectiveness of AI security risk management. Organizations should invest in AI-driven security tools that automate threat detection, response, and mitigation. Integrating these tools into CI/CD pipelines ensures that security checks occur throughout the AI development lifecycle, reducing vulnerabilities early. Automated systems can respond in real-time to security incidents, ensuring faster containment and reduced AI security risk.

4. **Invest in Relevant Capabilities:** To keep teams ahead of emerging AI security risks organizations should invest in evergreen upskilling teams and foster a culture of continuous learning through tactics like regular certifications and advanced workshops on emerging AI security trends.

    - Technical Competencies for Upskilling Initiatives: Cybersecurity fundamentals like threat modeling, secure coding practices, and

adversarial attack mitigation, DevSecOps, advanced encryption techniques, secure AI model deployment, and handling Model Drift and Concept Drift.

- Non-Technical Competencies for Upskilling Initiatives: Risk management, AI regulatory compliance (GDPR, CCPA), ethical AI practices, data privacy laws and basic cybersecurity awareness.

5. **Deploy a Security Champion Program:** Nominate security champions to drive awareness campaigns that educate employees on AI-specific security risks and best practices. Empower these champions to own initiatives like code reviews, security audits, regular knowledge sharing, and feedback loops across teams. Enable champions to drive formal coordination across AI, security, and IT stakeholders and to identify relevant protocols that should be implemented across teams.

6. **Unlock Resilience and Adaptability:** AI security strategies must be designed to continuously evolve in response to future threats and technological advancements. Resilience should be an intentional part of the security architecture, allowing organizations to adapt quickly to changing conditions. Several technical interventions can help drive greater AI security resilience:

- Redundancy Mechanisms: Use redundant systems and multi-cloud infrastructures to ensure operational continuity, avoiding single points of failure during outages or attacks.

- Self-Healing Systems: Leverage self-healing infrastructures for automated vulnerability detection and patching, reducing downtime and preventing future exploits without manual intervention.
- Dynamic Threat Modeling: Implement real-time threat modeling tools to continuously assess vulnerabilities, adjusting defenses proactively based on evolving threats.
- Adversarial Training for Models: Use adversarial training to fortify AI models against data poisoning, model evasion, and adversarial attacks; further refine models with adversarial examples.
- Scalable and Elastic Security: Design scalable security architectures using containerization and orchestration (e.g., Kubernetes) to dynamically adjust to system demands and growing threats.
- Cyber Resilience Playbooks: Develop cyber resilience playbooks with predefined responses for various incidents, using automated response orchestration to enable rapid mitigation and recovery.
- Continuous Learning for AI Models: Deploy continuous learning systems to update models with new data, ensuring they adapt to both known and emerging threats while maintaining accuracy.

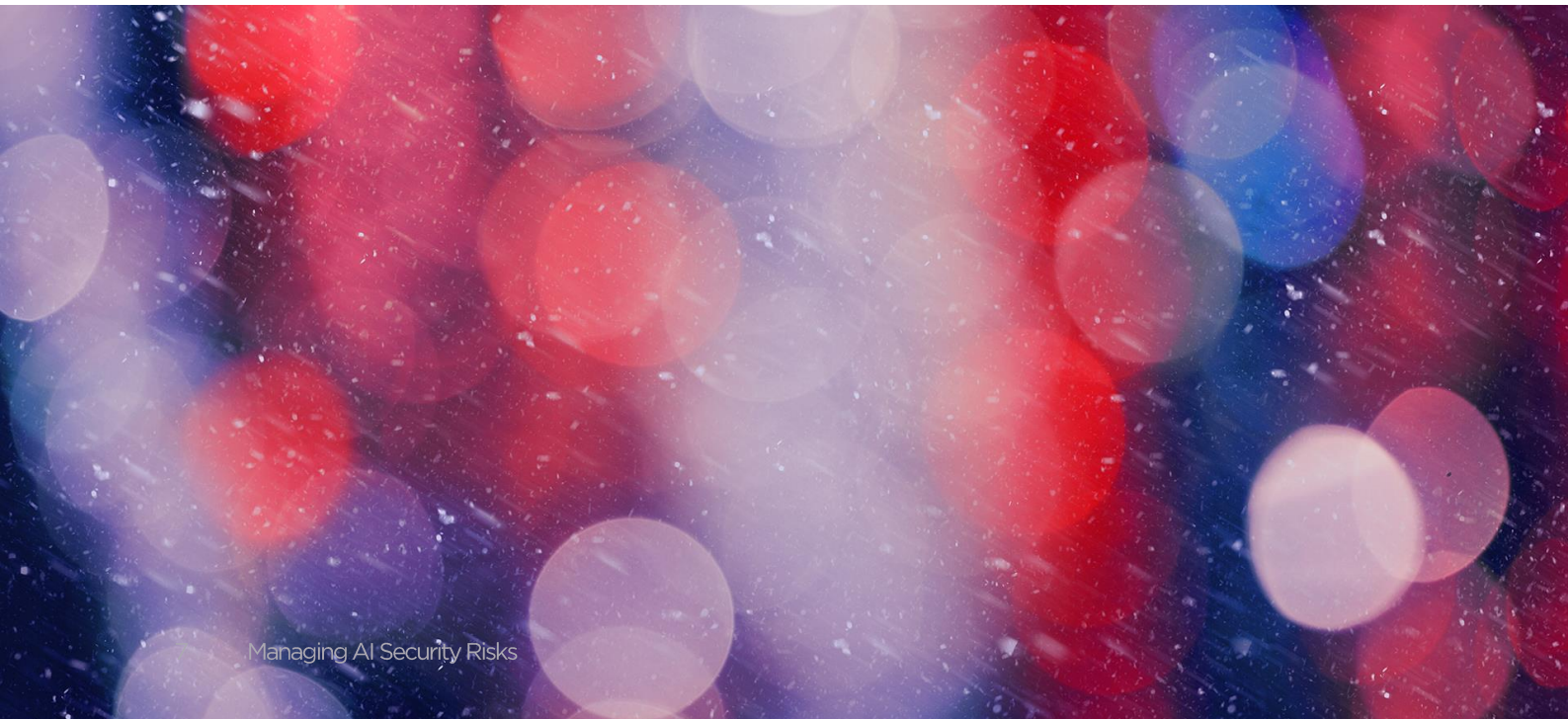
The shift to self-healing systems, dynamic threat modeling, and adversarial training makes resilience a core component of AI security and enables more

rapid responses to evolving threats.

While security concerns are real, the benefits of AI adoption far outweigh the risks when managed effectively. AI is a transformational technology that enables organizations to automate complex processes, drive innovation, and improve operational efficiency. By unlocking predictive insights and streamlining decision-making, AI offers significant advantages that can fuel growth and create competitive edges. However, these benefits must be balanced against the unique security challenges AI presents.

The key to achieving this balance lies in adopting a comprehensive AI Security Risk Framework. This framework enables organizations to proactively identify and mitigate risks such as model integrity issues, data breaches, and adversarial attacks. More importantly, it integrates security into broader business objectives, aligning AI deployments with organizational goals and regulatory standards, such as GDPR and CCPA.

AI security must be a tailored, multi-layered approach. By embedding security measures at every stage of the AI lifecycle, organizations can minimize vulnerabilities and maintain system integrity. Proactive strategies like continuous model monitoring, adversarial training, and ZTA help reduce attack surfaces while automated incident response systems ensure rapid containment of threats without disrupting business operations. Implementing AI security solutions also fosters broader benefits beyond risk mitigation. By building resilience into AI systems, businesses can confidently scale their AI initiatives, knowing that vulnerabilities are managed from the outset. This approach not



only accelerates innovation but also enables organizations to stay competitive and unlock new revenue streams, enhancing the overall return on AI investment.

Security should be viewed as a strategic enabler for AI adoption. As AI continues to revolutionize industries, securing AI systems is essential for maintaining trust with customers, partners, and regulators. The AI Security Risk Framework allows organizations to ensure AI deployments are not only secure but also fair, transparent, and accountable—key elements in building long-term customer loyalty and protecting brand integrity. Ultimately, the right security protocols empower businesses to harness AI's full potential without compromising safety. By implementing a proactive, multi-layered security framework, ITDMs and CISOs can ensure that AI adoption accelerates innovation, improves efficiency, and creates lasting competitive advantages. With AI poised to play an even greater role in business strategy, those who adopt strong AI security frameworks today will be best positioned to lead in tomorrow's digital economy.

In conclusion, adopting AI is not just about managing risks but about unlocking tremendous value. Organizations that embrace AI with robust security measures in place will gain a significant competitive edge, achieving the agility, innovation, and scalability needed to thrive in an AI-driven future. The AI Security Risk Framework is key to realizing this potential while maintaining the trust and security necessary for sustained success.

Getting Started

As AI continues to transform business operations, a robust and adaptive AI Security Risk Framework is crucial. The suggested actions below provide a tactical way for ITDMs and CISOs to get started or to strengthen their AI security postures.

Near Term Opportunities (Achievable in the Next 30 Days):

1. Conduct a Baseline AI Security Audit: Perform an initial security audit to identify high-risk vulnerabilities in AI models and data pipelines, focusing on enterprise-level devices and scalable infrastructure solutions that require specialized hardware and cloud integration. Prioritize quick fixes for critical systems.
2. Kickstart DevSecOps Integration: Begin integrating security scans into the AI development lifecycle, particularly in environments that rely on secure hardware for model training and deployment, ensuring tight integration with device management platforms and cloud services.
3. Implement Basic SIEM Alerts: Set up SIEM alerts for AI systems to monitor suspicious activity, with emphasis on enterprise devices and infrastructure that leverage AI for automation and scalability. Monitoring should cover both endpoint devices and centralized infrastructure.
4. Apply Zero Trust to Key Systems: Introduce multi-factor authentication and least privilege access for AI systems, with specific application to distributed devices and cloud infrastructure, ensuring tight access control across a wide network of commercial devices.
5. Organize AI Security Training: Hold an introductory security training session for teams managing enterprise devices and AI-driven solutions, with a focus on securing AI workflows in large-scale environments that integrate hardware and cloud services.
6. Identify and Assign Security Champions: Designate security champions within AI and IT teams who specialize in securing commercial devices and infrastructure solutions, driving security awareness and practices in complex, large-scale systems.
7. Foster Cross-Team Collaboration: Set up collaboration meetings between AI, IT, and security teams to align on securing AI-driven devices and enterprise infrastructure solutions, ensuring holistic security across the entire ecosystem.

AI Security Risk

As AI continues to evolve, a proactive and adaptive approach for AI security will be essential for maintaining operational integrity and regulatory compliance. The AI Risk Security Framework provides a holistic approach for mitigating evolving security risks and enabling organizational resilience considering an increasingly complex threat landscape.

References

[1]Gartner: AI-Enhanced Malicious Attacks Are a New Top Emerging Risk for Enterprises
[2]Forrester: Securing Generative AI
[3]Deloitte: Now Decides Next
[11]Lenovo US: CIOs perspectives of AI

About Lenovo

Lenovo is a US$57 billion revenue global technology powerhouse, ranked #248 in the Fortune Global 500, and serving millions of customers every day in 180 markets. Focused on a bold vision to deliver Smarter Technology for All, Lenovo has built on its success as the world's largest PC company with a pocket-to cloud portfolio of AI-enabled, AI-ready, and AI-optimized devices (PCs, workstations, smartphones, tablets), infrastructure (server, storage, edge, high performance computing and software defined infrastructure), software, solutions, and services. Lenovo's continued investment in world-changing innovation is building a more equitable, trustworthy, and smarter future for everyone, everywhere. Lenovo is listed on the Hong Kong stock exchange under Lenovo Group Limited (HKSE: 992) (ADR: LNVGY).