Pillar Technology
PARTNERS

THE CYBERSECURITY RISKS OF AI

Protecting your organization in the age of intelligent systems

Artificial intelligence (AI) is transforming industries, revolutionizing business operations, and driving efficiency like never before. However, as AI systems become more integrated into critical functions, they introduce significant cybersecurity risks. From adversarial attacks to data privacy concerns, organizations must proactively manage these threats to ensure AI is a tool for progress rather than a liability.

Security leaders—CIOs and CISOs—must develop AI strategies that balance innovation with security, ensuring AI augments rather than replaces the workforce. According to **Gartner**, nearly **90% of enterprises** are still in the research or piloting phase of **Generative AI (GenAI)**, with most lacking proper trust, risk, and security management policies. This signals an urgent need for security-focused AI governance.

This e-book explores the cybersecurity risks of implementing AI, detailing real-world case studies from healthcare, manufacturing, and financial services. We will also outline strategies to mitigate these risks and safeguard AI-driven systems.

Cybersecurity Risks of AI

Data Privacy & Confidentiality Risks

- AI systems process vast amounts of sensitive data, including personal and financial information.
- Improper data handling, unintentional exposure, or breaches can lead to significant security incidents.

Adversarial Attacks & AI Manipulation

- Attackers can exploit AI models by feeding them manipulated inputs designed to deceive them. This can lead to incorrect decisions in security-sensitive applications like fraud detection and medical diagnostics.

Bias, Discrimination & Hallucinations

- AI models can unintentionally reinforce biases, generating misleading or discriminatory outputs. Hallucinations—when AI produces completely false information—can pose security threats if relied upon for decision-making.

Malicious Use of AI in Cybercrime

- Cybercriminals are leveraging AI to automate phishing attacks, generate deepfakes, and launch sophisticated cyberattacks at scale, making traditional security defenses less effective.

Insider Threats & AI Misuse

- Employees may misuse AI systems for personal gain or inadvertently expose vulnerabilities by improperly configuring AI-driven security tools.

Poor Governance & Accountability

- Lack of clear policies on AI deployment and responsibility can lead to security risks. Unauthorized AI use within organizations can introduce vulnerabilities.

AI System Failures & Over-Reliance

- Over-reliance on AI-driven automation without human oversight can result in operational failures. When AI fails, entire systems may be left vulnerable.

Top 3 AI Security Concerns for Cybersecurity Leaders

Based on Gartner's research, security leaders cite the following as their primary AI-related security concerns:

Third-party access to sensitive data

- Unmanaged use of GenAI can lead to data leakage through third-party applications.

AI application and data breaches

- Poorly secured AI implementations introduce new vulnerabilities.

Erroneous decision-making

- AI can make flawed security decisions if models are manipulated or trained on biased/incomplete data.

Regulatory Compliance & AI Security

The Importance of Compliance with Regulatory Requirements

AI-driven systems must align with global data privacy regulations such as the:

- **General Data Protection Regulation (GDPR)**
- **California Consumer Privacy Act (CCPA)**
- **Emerging AI-specific laws**

Compliance ensures that organizations minimize security risks while maintaining transparency, fairness, and data protection.

Key Compliance Measures for AI Security

Organizations should:

Ensure AI models comply with **data protection and privacy laws.**

Implement **data minimization and encryption** practices to protect sensitive information.

Establish mechanisms for **user consent management** when processing personal data.

Maintain **audit trails** for AI decision-making to support regulatory inquiries.

Regularly review and update AI systems to align with **evolving regulations.**

Monitoring AI Regulations

AI regulations are constantly evolving.
Organizations must stay ahead by:

Appointing a **Regulatory Compliance Officer** to oversee AI legal obligations. (Some organizations are even appointing Chief AI Officers)

Subscribing to **industry and government AI regulatory updates**.

Engaging with **AI ethics and compliance organizations**.

Conducting **annual compliance audits** to identify and address gaps.

Failure to comply with AI-related regulations can lead to financial penalties, reputational damage, and increased security vulnerabilities, making compliance a key pillar of AI cybersecurity strategy.

Adapting AI Governance to Global Compliance Trends

As AI capabilities evolve, so too must the frameworks used to govern them. Adaptive AI governance aligns with emerging standards such as the **EU AI Act**, which emphasizes risk classification, transparency, human oversight, and accountability.

Organizations should integrate regulatory intelligence into their governance programs to ensure ongoing compliance and resilience.

- Incorporate regulatory scanning into your AI risk management
- Ensure governance frameworks can adapt to constantly-evolving international standards
- Ensure real-time compliance reporting capabilities
- Prioritize documentation and explainability of AI systems

Checklist: AI Risks to Watch

Data Privacy & Confidentiality

Sensitive Data used in AI training can unintentionally go public.

Adversarial Attacks

Cleverly disguised inputs can trick AI into making bad decisions.

Bias, Discrimination & Hallucinations

AI can unknowingly reinforce biases-or worse, generate completely false information.

Malicious Use of AI

From deepfakes to automated phishing. AI's dark side is evolving quickly.

Insider Threats

Employees may misuse AI systems for personal gain or malicious purposes.

Regulatory Non-Compliance

AI regulations are rapidly evolving, and non-compliance could result in significant penalties.

AI System Failures & Over-Reliance

When AI falters, it can bring operations to a standstill.

Poor Governance & Accountability

Without clear responsibilities, unapproved AI usage can introduce risk.

Healthcare: AI in Medical Diagnosis and Data Privacy Threats

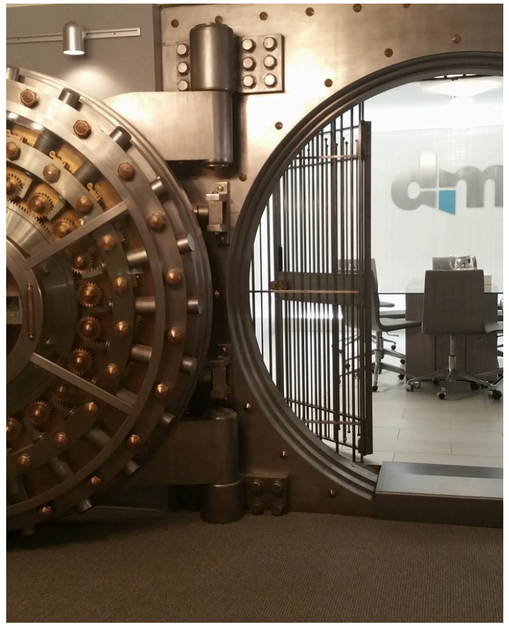
AI-powered diagnostic tools are improving healthcare efficiency, but they also pose risks. In 2024, a major hospital system suffered a data breach when attackers exploited an AI-driven patient data processing tool, exposing thousands of medical records. The breach highlighted the importance of securing AI models against unauthorized access and ensuring patient privacy.

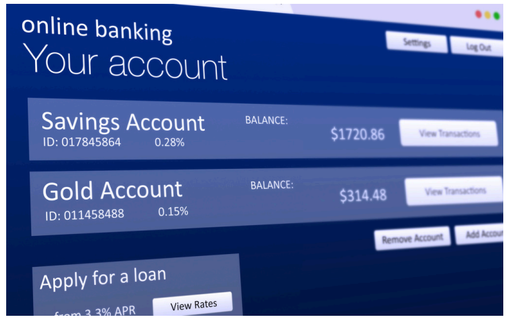
Manufacturing: AI-Driven Automation and Supply Chain Attacks

Manufacturers rely on AI for predictive maintenance and automated supply chain management. However, a 2025 cyberattack demonstrated the risks when an adversary manipulated an AI model predicting machine failures, causing unexpected downtime and financial losses. Attackers leveraged adversarial AI techniques to deceive the system, leading to incorrect operational decisions.

Financial Services: AI in Fraud Detection and Adversarial Manipulation

AI plays a critical role in fraud detection, but cybercriminals are evolving their tactics. In a high-profile case, fraudsters used adversarial machine learning to bypass an AI-powered fraud detection system, successfully laundering millions before detection. This case underscored the need for adaptive security measures that can respond to evolving AI-driven threats.





Roles in AI Security Leadership

Business Leaders

- Define business use cases for AI

CIOs

- Set AI strategy, align AI initiatives with business goals, and oversee adoption

CISOs

- Assess AI security risks, implement cybersecurity controls, constantly monitor the AI risk landscape and ensure compliance with rapidly-evolving compliance requirements

Data & Analytics Leaders

- Utilize AI to deliver meaningful analytics and business information to the organization

Enterprise Architects & Engineering Leads

- Develop AI infrastructure plans and ensure technology investments align with security needs
- Establish AI engineering best practices and secure AI applications

STRATEGY INSIGHT

AI's potential is immense, but so are its cybersecurity risks. As AI continues to advance, organizations must adopt a proactive approach to secure their AI-driven systems. By implementing strong governance, robust security measures, and a culture of AI awareness, businesses can harness AI's benefits while minimizing security threats.

Organizations must prioritize AI security to build resilience against emerging threats. Now is the time to assess AI security frameworks and ensure that AI remains a force for progress, not vulnerability.

Contact Us

For a deeper look at how to secure your organization's AI environment Pillar offers a free AI Discovery Session. Security starts with a conversation, contact us at:

678-304-9099

info@ptechcyber.com

www.ptechcyber.com

YOUR TRUSTED PARTNER IN MID-MARKET CYBERSECURITY

Pillar Technology
PARTNERS