Guidehouse®

A CISO's Guide to AI Privacy Risks

How to identify common AI privacy concerns, and what CISOs can do to mitigate AI and data security vulnerabilities.

As information technology evolves, organizations across every industry have been rushing to adopt and implement artificial intelligence (AI). But addressing AI privacy risks and mitigating bias entails more than just technical acumen—these problems cannot be solved by simply hiring more data scientists or writing more code. Designing AI models that work for people and organizations requires dedication to responsible automation. This involves commitment from governance at the highest levels, as well as teams that build responsible AI concepts into every new automation initiative.

While AI can deliver a wealth of transformational benefits to organizations, AI privacy concerns should be considered with as much care as the opportunities. Current AI risks and cybersecurity issues include data leakage and theft, legal compliance issues, inaccuracy and misinformation, biases, AI model targeting, human error and misuse, and supply chain vulnerabilities, among others.

This is the case across the private and public sectors alike. While the two may be at different stages of AI maturity, AI privacy risks are equally important across both sectors in unique ways.

For instance, the private sector tends to be more concerned with litigation in the event of security problems, along with potential financial and reputational impacts. The public sector is focused on maintaining compliance and facing different types of cybersecurity attacks from foreign threats.

Pressure to Adopt Is Compounding AI Privacy Issues

When managing complex AI technology implementations, CISOs have faced challenges in maintaining cybersecurity and data privacy best practices. In many cases, the urgency to adopt and deploy AI solutions has been so intense that some CISOs are understandably struggling to recognize the severity of AI privacy risks.

It's easy to see why, as the opportunities with AI are vast and the pressure to leverage them ahead of or at pace with competitors is significant. In many organizations, there has been little time to take a step back and consider designing and implementing a cybersecurity strategy specifically for AI.

The perception is that the more data AI platforms receive, the better the results the business can gain.

How Sensitive Data Becomes at Risk

With AI technology, the goal is for the models to ingest as much data as possible. The perception is that the more data AI platforms receive, the better the results the business can gain. This may lead to entering sensitive, high-profile customer and third-party data like health data, biometric data, or personally identifiable information, into AI platforms without sufficient consideration for data privacy or cybersecurity. The resulting risks include:

Privacy concerns due to speed of data processing: AI's ability to rapidly process vast quantities of data from multiple sources can allow previously anonymized data to become identifiable once cross-referenced.

Reduced data input awareness: The rush to maximize data input can leave executives without full visibility into the data their AI model contains, limiting their ability to accurately assess risk.

Tensions between workforce capabilities and security: Executives can feel that limiting data inputs to mitigate risks will constrain their workforce from maximizing AI benefits.

A lack of AI privacy policy maturity: Robust AI data privacy regulations may not yet provide effective guardrails for AI privacy risk and may need further refinement.

Awareness and Education Can Reduce Risk

To remain comprehensively protected in the age of AI, CISOs should foster a cultural shift toward a more security-conscious, risk-aware organization. Mitigating AI privacy risks will require investment to train and educate staff on how to maintain data security and privacy with AI, including the C-suite.

CISOs must also take proactive steps to future-proof their security posture through continual learning and organizational development. As AI is evolving so quickly, many AI privacy risks are likely yet to emerge, so CISOs must ensure they stay ahead of potential cybersecurity threats.

With data privacy management, it's also important for CISOs to help decision-makers understand the implications of any downstream companies, partners, or other parties within the value chain who may be able to access—and, as a result, compromise—AI tools containing sensitive data. This is especially important for government agencies with a lot of interdepartmental collaboration across systems.

A Blueprint for Mitigating AI Privacy Risks

It's crucial for CISOs to evolve their AI cybersecurity and data privacy management practices. CISOs must prioritize AI data privacy risks alongside the opportunities and communicate the relevant security best practices throughout the organization.

Introducing cybersecurity and data privacy best practices into AI-related programs requires strategic steps:

- Take a risk-based approach to data protection and data privacy and establish a dedicated AI risk management program. This involves identifying what data the organization currently has or plans to acquire and what the impacts would be if that data were to be compromised. Tools including risk management assessment frameworks, data models, and asset intelligence reports can help facilitate this process.
- Determine the organization's risk tolerance and understand where the priorities are. Guidehouse experts recommend a zero-tolerance risk policy regarding data privacy, especially with AI tools.
- Strengthen parallel enterprise risk management programs to ensure the organization's cybersecurity posture is as strong as possible. This may involve adopting risk management technologies and improving risk governance processes, like risk response decision-making.
- Gain up-to-date intelligence and inventory on what data CISOs have, what data has been ingested by their large language models, the impact of this data being compromised, and what needs to be done to reinforce data protection.
- Manage AI privacy risks through privacy by design, an approach wherein CISOs proactively consider privacy and security before implementing a tool, rather than reactively addressing issues post-implementation.

CISOs must prioritize AI data privacy risks alongside the opportunities and communicate the relevant security best practices throughout the organization.

Organizations must manage the urgency to deploy AI at speed while working to mitigate the vulnerabilities involved with AI and data security.

CISOs across all industries should develop a comprehensive summary of sector-specific concerns and AI risks. For example, healthcare organizations will need additional cybersecurity and data privacy measures for biometric data. Financial services companies will need to do the same with such sensitive data as social security numbers and income data. CISOs should proactively seek new guidance and recommendations from industry leaders and governing bodies.

Finally, it will become increasingly important to build cross-functional teams and empower collaboration with experts across departments to develop truly secure organizations. This will enable privacy teams, security teams, enterprise risk management teams, and other technology teams to work together to maximize resilience.

Building a More Secure, Innovative Organization

Organizations across both the public and private sectors must manage the urgency to deploy AI at speed while working to mitigate the vulnerabilities involved with AI and data security, taking a zero-tolerance policy when it comes to risks.

Doing so will provide far greater peace of mind throughout the organization and minimize the risk of potentially catastrophic data breaches. This will ultimately allow technology leaders to focus entirely on innovation, using secure, protected data to leverage AI to its full potential.

Contact Guidehouse to learn how our AI privacy experts can help your organization manage AI privacy risks.

Contacts

Amanda Kane, Partner
Defense & Security – Cybersecurity
amkane@guidehouse.com

About Guidehouse

Guidehouse is a global consultancy providing advisory, digital, and managed services to the commercial and public sectors. Guidehouse is purpose-built to serve the national security, financial services, healthcare, energy, and infrastructure industries. Disrupting legacy consulting delivery models with its agility, capabilities, and scale, the firm delivers technology-enabled and focused solutions that position clients for innovation, resilience, and growth. With high-quality standards and a relentless pursuit of client success, Guidehouse's more than 17,000 employees collaborate with leaders to outwit complexity and achieve transformational changes that meaningfully shape the future. guidehouse.com.

guidehouse.com/services/cybersecurity

GHTechSolutions

linkedin.com/showcase/guidehouse-technology-solutions