VIEW POINT

ENSURING DATA SECURITY IN A DEMOCRATIZED GENERATIVE AI LANDSCAPE

Infosys®
Navigate your next

Overview

Enterprises are constantly seeking innovative strategies to maintain their competitiveness in an era of rapid technological advancement. Among the transformative forces at play, Generative Artificial Intelligence, or Gen AI, has emerged as a disruptive game-changer. As per Gartner, by 2026, Gen AI will significantly alter 70% of the design and development effort for new web and mobile applications. Leveraging its capabilities to automate processes and generate content, Gen AI is reshaping a multitude of industries. However, the swift integration of Gen AI into commercial operations brings to the forefront, a host of data security concerns that must not be underestimated.

The POV delves into these concerns with a comprehensive exploration and identify potential solutions. The author analyzes the multifaceted impact of Gen AI on data security, addressing the intricate challenges that businesses face while navigating this transformative landscape. By doing so, the author aims to provide insights and strategies that will enable enterprises to harness the potential of Gen AI while safeguarding their valuable data assets.

Data Security challenges in the Gen AI adoption

- **Privacy of data and adherence to regulations**

  Enterprises have amassed extensive datasets that encompass a wealth of customer information and sensitive business data. The utilization of such data for training AI models gives rise to substantial privacy considerations. Striking an optimal equilibrium between innovation and the preservation of data privacy proves to be a formidable challenge. The potential ramifications of failing to achieve this balance are multifaceted and significant. One primary concern lies in the potential damage to the enterprise's reputation. Mishandling or neglecting data privacy can erode trust and goodwill among customers and partners. Additionally, legal consequences loom large, with the possibility of substantial fines and legal penalties if the enterprise falls afoul of data protection regulations such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act).

- **Unauthorized access and data breach**

  Gen AI systems require large datasets, but there is a risk of data loss or unauthorized access. If sensitive information is not adequately protected, it may be accessible to external actors or even internal personnel with malicious intent. Personal data, like names, addresses, and contact details, can be inadvertently collected during interactions with AI systems. The processing of personal data by Gen AI algorithms may result in unintended exposure or misuse of this information.

- **Addressing bias and fairness in AI**

  The data that is used to train AI models is often biased, reflecting the biases of the people and systems that created it. For example, if an AI model is trained on a dataset of images that are predominantly white, the model may be more likely to classify white people as people and black people as objects. This bias can be perpetuated in the AI models themselves. Once an AI model is trained on biased data, it will start to reflect those biases in its own predictions, leading to discriminatory or unjust outcomes. Businesses that are using AI need to have procedures in place to detect and reduce bias in their AI systems.

- **Risks of insider threats:**

  Insider threats refer to the risks posed by employees who have access to AI systems and may abuse them for their own gain or accidentally compromise data security. While external risks are typically higher, internal threats cannot be ruled out in an organization. To reduce these hazards, effective monitoring and access controls are crucial. Insider threats can occur due to negligence, lack of cyber awareness, or sheer malice. Organizations must prioritize transparency and user consent to ensure individuals understand the data collection and processing activities associated with AI systems.

- **Holding accountability:**

  AI systems are often complex and opaque, making it difficult to hold them and their creators accountable for data security breaches or other problems. This can be a significant challenge for organizations that rely on AI systems to process sensitive data and make critical decisions. The lack of accountability can lead to unintended consequences, such as perpetuating discrimination or resulting in unjust judgments.

Key strategies to mitigate Data Security concerns with Gen-AI

As Gen AI continues to gain popularity, it is essential to take the necessary steps to mitigate potential data security and privacy risks. Here are some strategies to consider:

- **Addressing Data Security risks with Gen AI**

  To mitigate data security concerns with Gen AI, it is crucial to put in place a strong data governance framework that includes data classification, encryption, access controls, and auditing. This framework ensures consistency, security, and compliance throughout the Gen AI process. Data governance is a fundamental aspect of data management for Gen AI, and it involves establishing a framework of policies and procedures to guide data collection, storage, and use. To protect sensitive information, it is essential to make sure that data used to train Gen AI models is anonymized and aggregated whenever possible. By implementing a robust data governance framework, businesses can ensure the responsible and ethical use of Gen AI while maintaining regulatory compliance.

- **Collaborate with trustworthy Gen AI vendors**

  To mitigate data security concerns with Gen AI, enterprises should consider using Gen AI providers that have a good track record of security and privacy. It is essential to review the provider's security documentation and policies to ensure that they meet the organization's needs. This is especially important when dealing with sensitive data, such as personal and financial information. Companies should also consider conducting due diligence before entrusting their personal information to a Gen AI service.

- **Create a trusted environment**

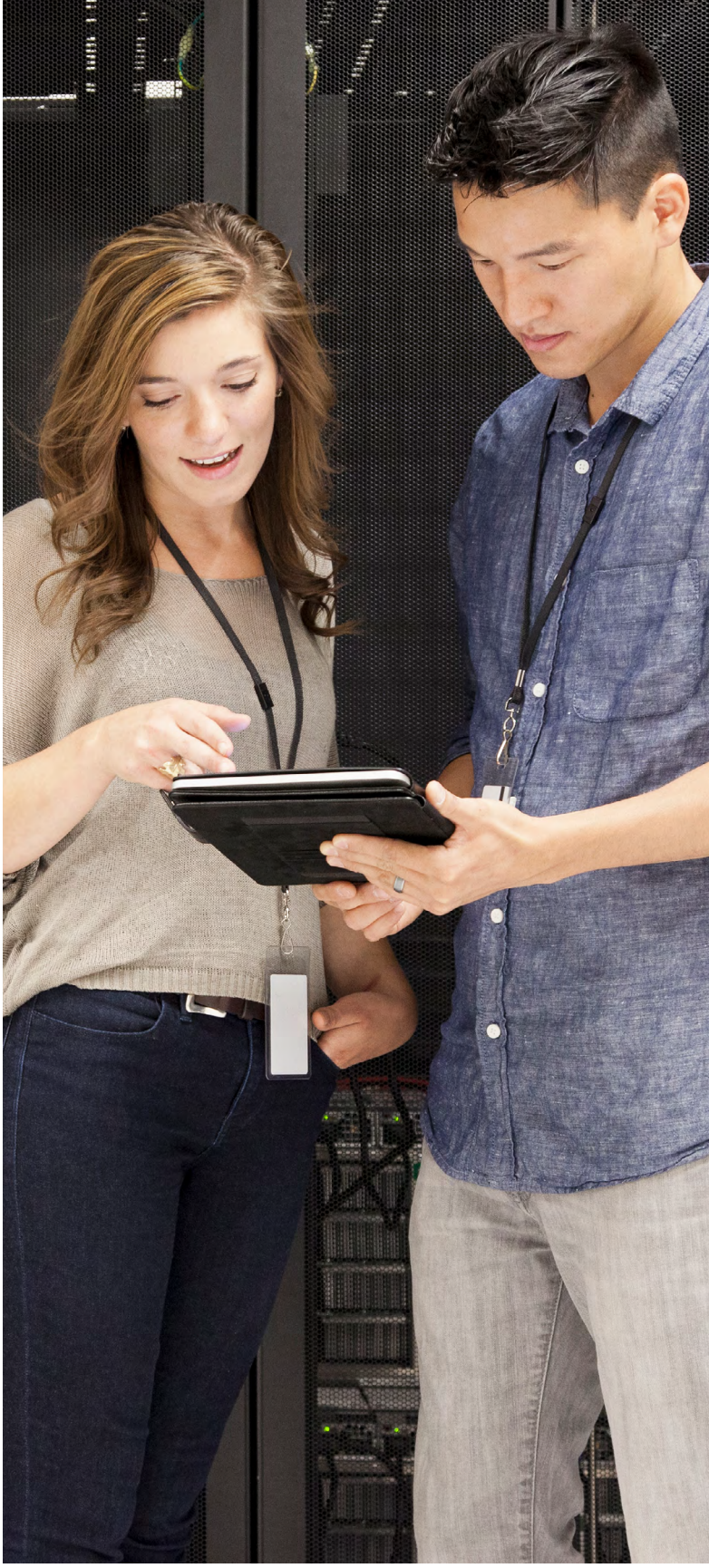
  Creating a trusted environment and minimizing the risk of data loss is essential. it is important to educate employees on data security best practices, data leakage concerns, and the significance of ethical AI usage. This can be achieved by providing comprehensive training to all employees who interact with Gen AI. Organizations should start training their employees on Gen AI security risks and create internal usage policies.

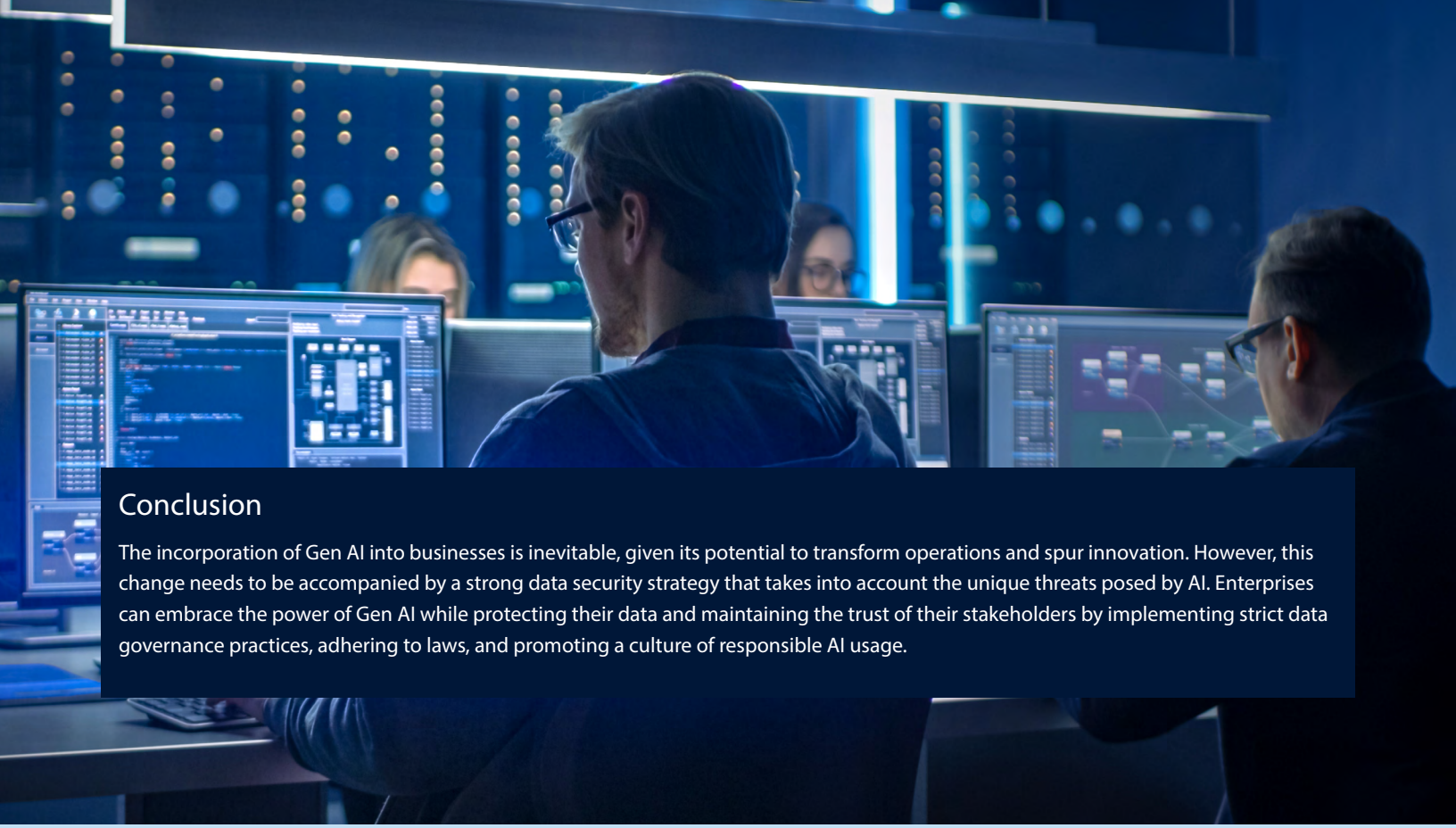
- **Secure the entire AI pipeline**

  Focus on securing and encrypting the data used to train and tune AI models. Continuously scan for vulnerabilities, malware, and corruption during model development, and monitor for AI-specific attacks (e.g., data poisoning and model theft) after the model has been deployed. Collaboration with cybersecurity experts and AI ethics professionals are imperative, to assess and enhance the security of Gen AI implementations. These experts can provide valuable insights into potential vulnerabilities and areas of improvement. Seeking external audits and ethical reviews of AI systems can also help identify potential risks and vulnerabilities.

- **Safeguarding sensitive information**

  To mitigate data security concerns with Gen AI, businesses should prioritize data security, implement encryption, DLP, Pseudonymization and other robust security measures, use sensitive data protection, adhere to data protection regulations, establish ethical AI practices, and seek external audits. By implementing these strategies, businesses can ensure that their Gen AI applications are secure and compliant with regulatory requirements.





Conclusion

The incorporation of Gen AI into businesses is inevitable, given its potential to transform operations and spur innovation. However, this change needs to be accompanied by a strong data security strategy that takes into account the unique threats posed by AI. Enterprises can embrace the power of Gen AI while protecting their data and maintaining the trust of their stakeholders by implementing strict data governance practices, adhering to laws, and promoting a culture of responsible AI usage.

Author

Saurabh Sharma

Saurabh works as a Data Privacy & Protection Consultant with Infosys Cyber Innovation Strategy and Excellence team which dwells into next generation cyber security solutions and strategies. He has 13 years of experience in consulting, assessment & implementation of data protection and building data privacy solutions. He has extensive knowledge and experience in Infrastructure and Cloud Security domains as well.

References

https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2024

https://hbr.org/2023/06/managing-the-risks-of-generative-ai

https://www.cio.com/article/482235/7-key-questions-cios-need-to-answer-before-committing-to-generative-ai.html

https://www.linkedin.com/pulse/data-management-generative-ai-success-john-giordani/

For more information, contact askus@infosys.com

Infosys®
Navigate your next