|  |  |
| --- | --- |
| Name: Advay Sharma | Project Title: Market Research |
| Service Line: Consulting | Role: Intern |

*Task 3*: As manufacturing and financial services organizations increasingly adopt AI for operational efficiency, what are the potential technology-related risks they should be aware of, and what mitigation strategies can be employed to manage them?

*Sources:* IBM, Cognizant, and McKinsey

*Solution:*

Implementing AI in sectors like **manufacturing** and **financial services** is becoming the norm today, and for good reason — it brings speed, efficiency, and smart decision-making. But with all this promise, there are also a few key risks we need to be aware of, especially when AI is used in day-to-day processes.

**🚨 Common Risks When Using AI in Business Operations**

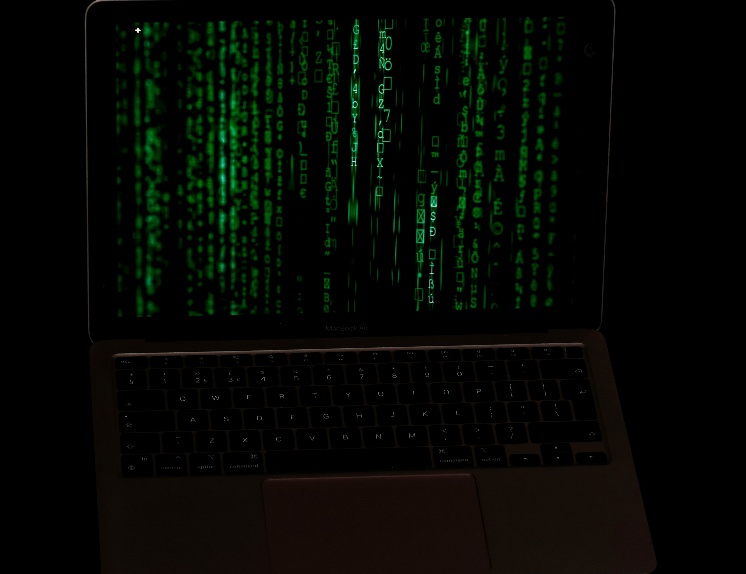
**1. Bias in Decision Making**

AI models learn from data — and if the data has hidden biases, the results can be unfair. For example, in banking, an AI might wrongly deny loans if it’s trained on biased historical data.  
👉 *How to handle it:* Make sure data sets are diverse and clean, regularly audit models, and build fairness checks into the process.



**2. Cybersecurity Vulnerabilities**

AI systems can be hacked or manipulated — this can be especially dangerous in manufacturing, where a compromised AI could stop or misdirect production. Similarly, in finance, it could open doors to fraud.  
👉 *How to handle it:* Treat AI like any critical tech asset — secure it with encryption, regular testing, and real-time monitoring.



**3. Privacy Issues**

Since AI thrives on large volumes of data, privacy becomes a concern. Financial data, in particular, is sensitive. Mishandling it could lead to regulatory trouble and a loss of client trust.  
👉 *How to handle it:* Use anonymization, follow data protection laws like GDPR, and be transparent about how data is used.

**4. Regulatory and Compliance Gaps**

Laws are still catching up with AI. If a bank uses an AI tool that unintentionally discriminates, it could end up violating anti-discrimination laws without even realizing it.  
👉 *How to handle it:* Keep legal and compliance teams in the loop when building or deploying AI tools, and stay updated with evolving regulations.

**5. Operational Errors**

AI isn't perfect. If a model misfires — say, misjudging production output or making a bad investment call — it can be costly.  
👉 *How to handle it:* Don’t go “AI-only.” Combine machine intelligence with human oversight, and have fail-safes in place to catch mistakes early.

**✅ How Companies Can Stay Ahead of These Risks**

* **Set up a solid AI governance framework** — define responsibilities and policies from the start.
* **Regularly audit AI models** — check for fairness, explainability, and compliance.
* **Train employees** — so that business and tech teams understand how AI works and what to watch out for.
* **Collaborate with legal and compliance teams** — especially in sensitive areas like finance, healthcare, and data privacy.

The good news is — industry leaders like **IBM**, **Cognizant**, and **McKinsey** are already sharing best practices on how to manage these risks. For example:

* IBM talks about dangers like bias, misuse, and the importance of explainability.
* Cognizant highlights specific risks in banks and insurers using generative AI.
* McKinsey focuses on how companies can identify their *biggest* AI risks and build risk-aware strategies.

So overall, AI is powerful — but like any tool, it needs careful handling. With the right checks and balances, businesses can safely unlock its full potential without running into trouble.

*References:*

* IBM: <https://www.ibm.com/think/insights/10-ai-dangers-and-risks-and-how-to-manage-them>
* Cognizant: <https://www.cognizant.com/us/en/insights/insights-blog/how-banks-and-insurers-can-avoid-generative-ai-risks-wf2262551>
* McKinsey and Company: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/getting-to-know-and-manage-your-biggest-ai-risks>