PRUDENT
THE FUTURE OF INSURANCE

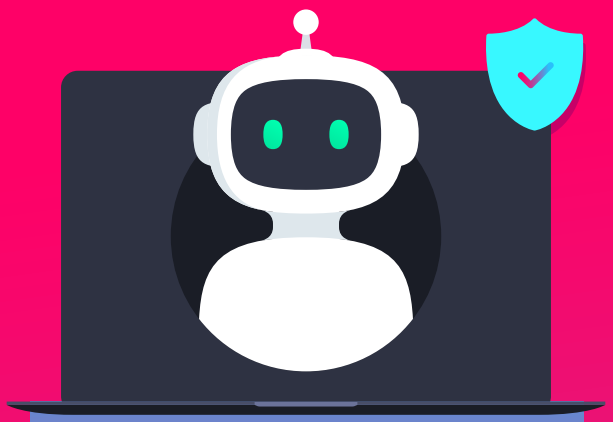
PARIMA
By Risk Managers For Risk Managers

THE GAME-CHANGING POWER OF ARTIFICIAL INTELLIGENCE

Redefine Risk Management

WWW.PRUDENTBROKERS.COM

Index:



1. Introduction

The incorporation of Artificial Intelligence (AI) into your business practices ushers in a new era of efficiency and competitiveness. By taking over repetitive and time-consuming tasks through workflow automation, AI allows you to streamline operations, reduce human error, and optimise business processes. According to a recent survey by Microsoft Azure, The State of AI Infrastructure report reveals that 95% of businesses plan to increase their AI usage over the next two years. [16]

This not only yields substantial cost savings but also enhances your customer experience by providing quick, intelligent solutions to their needs.

Incorporating AI to optimise business operations enhance the company's productivity, reduces operational costs, and streamlines workflows.

Below are a few examples:

Customer service with AI chatbots – Immediate 24/7 assistance to customers, answering FAQs, managing orders, etc. Allowing your human customer service to focus on more complex issues. [1]

Data-driven decision-making with predictive analytics – AI systems can analyse patterns in large datasets to forecast future trends and consumer behaviours. Organisations leverage this power to fine-tune marketing strategies, pricing, and product development. [1]

Inventory management – AI-driven forecasting tools can analyse sales data, seasonal trends, and economic indicators to provide precise inventory requirements. Example: **Zara** uses AI to forecast trends and manage inventory efficiently. [1]

Streamlining administrative tasks – automated scheduling, email sorting, and data entry not only save hours of manual labour but also minimise human error. [1]

Enhancing supply chain – with intelligent automation, demand prediction, optimisation of inventory levels, and dynamic pricing strategies facilitation. [1]

Automating financial procedures and reporting – AI algorithms provide predictive analytics for better financial planning, while automation ensures compliance and timely reporting. [1]

Implementing AI tools for marketing and sales – AI analysis tools interpret customer data to forecast trends and buying patterns, enabling you to craft campaigns that resonate profoundly with your audience. [1]

Business security and fraud detection – Advanced algorithms detect anomalies and potential threats in real-time, significantly reducing the risk of data breaches and fraud. Example: **PayPal** uses AI to detect and prevent fraudulent activities in its payment ecosystem. [10]

Enhanced product search – AI improves search algorithms to provide more relevant results, using Natural Language Processing (NLP) to understand the user intent. Example: **Google Shopping** uses NLP to refine search results and suggest relevant products.

Customer retention and re-engagement – AI identifies customers likely to churn and sends personalised offers or reminders to retain them. Example: **Shopify** offers tools for small businesses to analyse customer data and send targeted re-engagement emails. [17]

Content generation – AI creates product descriptions, ad copy, and marketing content, reducing manual effort. Example: **Alibaba** uses AI to generate product descriptions for its vast catalogue. [15]

Predictive modelling and simulation – AI creates predictive models to simulate real-world scenarios, saving costs and time in testing. Example: **Boeing** employs AI to simulate aircraft designs and optimise performance before physical prototyping. [14]

Optimising research processes – AI enhances workflows by identifying inefficiencies and suggesting process improvements. Example: **Siemens** uses AI to optimise energy consumption and efficiency in manufacturing R&D. [12]

Innovative product design – AI generates design ideas based on parameters like performance, material constraints, and environmental impact. Example: **Autodesk's** AI-powered generative design tools help engineers create optimised products for specific needs. [13]

Text mining and knowledge discovery – AI extracts valuable insights from scientific literature, patents, and other text sources. Example: **Google DeepMind** uses NLP to analyse medical literature for breakthroughs in healthcare research. [21]

Contrary to this, attackers can also leverage AI to enhance the efficiency of cyberattacks. AI-powered malware can adapt its behaviour to evade detection by traditional cybersecurity measures, making it more challenging to detect and defeat threats. AI-enabled cyberattacks are becoming more common and costly. Here are some statistics about AI-enabled cyberattacks:

AI-powered phishing attacks: Generating highly targeted phishing emails that mimic the writing style of a specific recipient's boss or company, increases the likelihood of them clicking malicious links. According to SlashNext, phishing attacks increased by 4,151% after ChatGPT's release in late 2022. [20.a]

Deepfake social engineering attacks: Creating realistic video or audio recordings of a trusted individual to trick users into revealing sensitive information. According to Deep Instinct, 61% of organisations saw an increase in deepfake attacks over the past year. [20.b]

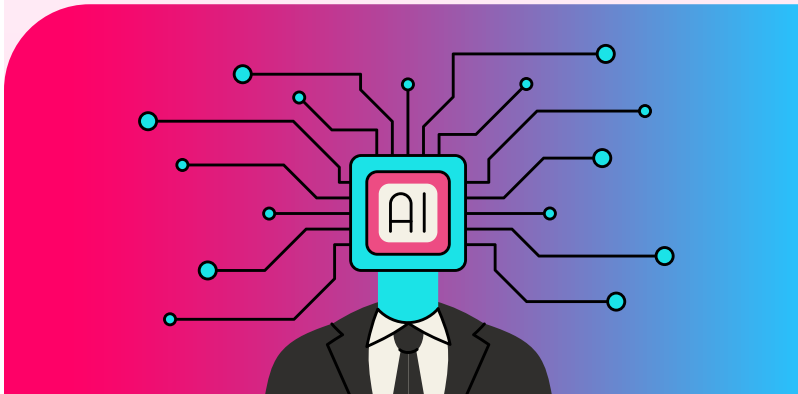
Generative AI: According to Deep Instinct, 85% of security professionals attribute the increase in attacks to generative AI. [20.c]

AI-powered malware: Using generative AI to create polymorphic malware that constantly changes its code to evade detection by traditional antivirus software. AI-powered malware can adapt to evade detection by traditional cybersecurity measures. [20.d]

Data poisoning and exfiltration: Intentionally feeding biased or incorrect data into an AI model to manipulate its decision-making process. Also deploying AI-powered chatbots that impersonate customer service representatives to trick users into divulging sensitive information. AI tools put companies at risk of data exfiltration. [20.e]

AI-driven reconnaissance: Using AI to analyse publicly available data on social media or other online sources to gather information about potential targets before launching an attack. [20.f]

AI-enhanced brute force attacks: Using AI to optimise password-cracking attempts by identifying patterns in common password combinations, significantly speeding up the process. [20.g]



2. Sectoral Use Cases of Artificial Intelligence

a. Financial Services

In the financial sector, AI is enhancing customer engagement and risk management. Below are the AI applications that streamline operations and improve customer satisfaction in the financial industry.

Notable implementations include:

- **Fraud detection –** AI analyses transaction patterns to identify and prevent fraudulent activities
- **Customer service –** chatbots and virtual assistants handle banking queries, reducing wait times
- **Loan processing –** AI automates the credit scoring process, enabling faster loan approvals
- **Risk management –** AI models predict market trends and assess portfolio risks more accurately
- **AI chatbots – HDFC Bank** employs AI chatbots for customer support, providing quick and personalised responses to queries
- **Credit scoring –** companies like **CreditVidya** use AI algorithms to assess creditworthiness, promoting financial inclusion by evaluating individuals without traditional credit histories

Example: **ICICI Bank** uses AI-powered voice bots to enhance customer experience in phone banking.

b. E-commerce

AI is revolutionising e-commerce by enhancing customer experiences, optimising logistics operations, and driving better decision-making. AI-driven insights enable personalised customer experiences and improve supply chain management.

Here's how AI is applied in various aspects of the e-commerce industry:

Personalised recommendations:

AI analyses customer behaviour, purchase history, and preferences to provide personalised product recommendations.

Example: **Amazon** uses AI to suggest products based on browsing and purchase patterns, increasing conversion rates and customer satisfaction. [19]

Chatbots and virtual assistants:

AI-powered chatbots provide 24/7 customer support, answer queries, and assist in purchase decisions.

Example: **H&M** uses a chatbot to help customers find the right size or style, improving user engagement. [18]

Dynamic pricing:

AI algorithms monitor competitor pricing, demand, and market trends to adjust prices in real-time, ensuring competitiveness.

Example: **Flipkart** uses dynamic pricing during sale events to optimise revenue. [19]

Visual search:

Customers upload an image to find visually similar products using AI-based image recognition.

Example: **Myntra** offers a visual search feature that helps users find fashion items based on photos. [18]

Fraud detection:

AI identifies fraudulent transactions and unusual behaviour, enhancing payment security.

Augmented Reality (AR) integration:

AI powers AR features that let customers visualise products before purchasing. Example: **IKEA** uses AR to help customers see how furniture fits in their homes.

Case study:
Amazon's AI in personalisation: Amazon's recommendation engine contributes significantly to its revenue. [40]

c. EdTech Sector

AI-powered CRM solutions are transforming the EdTech industry by automating lead scoring, personalising learning recommendations, and improving student retention. For instance:

Personalised learning recommendations:
AI analyses student behaviour and performance to suggest tailored courses or study materials, enhancing engagement and outcomes (on the basis of search and liked courses on the platform).

Automated lead scoring:
By evaluating engagement patterns, AI-driven CRMs prioritise high-potential students, ensuring timely follow-ups.

Predictive analytics for retention:
AI identifies students at risk of disengagement, enabling proactive interventions to improve retention rates.
These strategies have been effectively implemented by CRM providers like **Merrito, LeadSquared, Kylas, and TeleCRM** in collaboration with EdTech companies.

d. Manufacturing Industry

AI optimises production processes, reduces downtime, and enhances quality control through predictive analytics. For example:

Predictive maintenance:
Tata Steel utilises AI for predictive maintenance, reducing downtime and improving production efficiency.

Production optimisation:
AI analyses production line data to identify bottlenecks.

Quality control:
Vision-based AI systems inspect products for defects, ensuring consistent quality.
Example: **Hero MotoCorp** incorporates AI in its production lines to ensure consistent product quality, leading to better customer satisfaction.

e. Pharma and Healthcare

Research and development:
AI is transforming Research and Development (R&D) across industries by accelerating discovery, optimising processes, and enabling innovative approaches to problem-solving.

Drug discovery and development:
AI accelerates drug discovery by analysing large datasets to identify potential drug candidates and predict their efficacy.
Example: **Insilico** Medicine used AI to identify a new drug candidate for fibrosis in less than 18 months, a process that traditionally takes years.

Material science:
AI predicts properties of new materials and simulates molecular interactions, reducing the time required for experimentation.
Example: **DeepMind's AlphaFold** predicts protein structures with high accuracy, aiding research in biochemistry and materials science.

Personalised medicine:
AI analyses genetic data to recommend tailored treatments, enhancing patient outcomes.

Diagnostics:
AI systems assist doctors in detecting diseases like cancer from imaging scans with high accuracy.

Administrative automation:
Chatbots and AI-powered schedule systems streamline hospital operations.

Automated experimentation:
AI-powered robotics and algorithms automate complex experiments, improving efficiency and reducing human error.
Example: **IBM's RoboRXN** platform automates chemical synthesis using AI and cloud computing.

Data analysis and pattern recognition:
AI analyses massive datasets to uncover hidden patterns and insights, enabling informed decision-making.
Example: **NASA** uses AI to process astronomical data, identifying exoplanets and other celestial phenomena.

Clinical research optimisation
AI identifies suitable participants for clinical trials and monitors data in real-time to ensure accuracy and compliance.
Example: **Medtronic** uses AI to optimise clinical trials and improve the reliability of results.

Sustainability and environmental research:
AI helps develop sustainable solutions by modelling ecosystems, predicting climate change impacts, and optimising resource use.
Example: AI-driven tools from **Microsoft's AI** for the Earth initiative support research in conservation and environmental sustainability.

Case study:
Pfizer and IBM Watson: Pfizer uses IBM Watson's AI to identify immuno-oncology drug candidates. [41]

f. Infrastructure and Transport

Predictive maintenance:
AI systems monitor structural health, reducing infrastructure repair costs.

Traffic management:
AI analyses traffic patterns to optimise signal timings, reducing congestion.

Route optimisation:
AI-powered algorithms help transport companies plan the most efficient routes.

Smart parking:
AI systems guide drivers to available parking spots, enhancing user experience.

Example: **Delhi Metro** uses AI for predictive maintenance of trains and tracks, ensuring uninterrupted operations.

g. Media and Entertainment

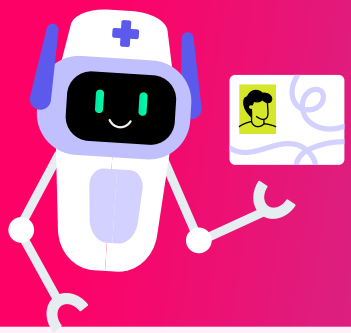
Content creation:
AI generates automated news summaries, subtitles, and even creative scripts.

Audience analysis:
AI analyses viewer preferences to recommend tailored content, increasing engagement.

Advertising optimisation:
AI optimises ad placements based on user behaviour analytics.

Post-production:
AI tools streamline video editing, animation, and visual effects production.

Example: **Zee5** employs AI to provide personalised viewing recommendations for its users.



3. Possible changes in the threat landscape

AI risks encompass potential harm to individuals, organisations, or systems arising from developing and deploying AI systems. These risks can result from various factors, including the data used to train AI, the AI algorithm, its use for multiple purposes, and interactions with people. Examples of AI risks and controls vary from biased hiring tools to algorithms causing market crashes.

Proactive monitoring of AI-based products and services is crucial to ensure the safety and security of data and individuals. Thus, organisations believe in employing a risk management solution that can help triage, verify, and mitigate these risks effectively.

AI offers immense potential to businesses but also brings significant risks with its implementation. To ensure responsible AI adoption, it is vital to understand and address these challenges at the right time. Further, let us look at the AI risks and solutions for businesses in detail.

Risk 1: Accuracy and Accountability

One of the most significant challenges in AI today is the issue of accuracy and accountability. Many AI systems are plagued by errors, stemming from unreliable data sources, non-transparent operations, and limited mechanisms for verification. These problems raise critical questions:

- **Where does the information come from?**
- **How can the data be verified?**
- **What are the origins and quality of the training datasets?**

Unfortunately, most AI applications function as "black boxes," meaning their inner workings are opaque. This lack of transparency undermines trust in their outputs, as users are unable to evaluate the reliability of the data or algorithms driving these systems. Borrowing from the intelligence community's principle of “trust but verify,” AI systems often fail to meet the verification requirement.

The inaccuracies of AI systems are not theoretical—they have been widely documented. Below are some notable examples of how AI's shortcomings in accuracy have led to real-world consequences:

- **AI in COVID-19 diagnostics:** During the pandemic, AI was expected to play a critical role in diagnosing COVID-19 to support healthcare providers. However, an evaluation of 415 AI tools found that none met the standards for clinical use. This failure not only highlights the gap between AI’s potential and its practical application but also underscores the risks associated with over-reliance on untested AI systems.
- **Zillow’s Real Estate AI:** Zillow, a leading real estate data company, suffered a $300 million financial loss when its AI-driven pricing algorithm failed to accurately estimate home values for its Offers Program. This example demonstrates the economic risks associated with inaccurate AI applications, particularly in high-stakes industries.

These are just a few examples – there are plenty more. Some of them present risks to financial and physical health. The question organisations need to ask: Do you trust AI without the appropriate supervision and testing?

Broader Implications

These examples underscore the widespread implications of AI inaccuracies:

- **Financial risks:** Errors in financial decision-making or market predictions can lead to significant economic losses, as seen in the Zillow case.
- **Physical and health risks:** Inaccurate AI systems in healthcare can jeopardise patient safety, as evidenced during the COVID-19 pandemic.
- **Professional risks:** When AI systems produce flawed recommendations or analyses, professionals relying on these tools (e.g., lawyers, doctors, or financial analysts) may face reputational and legal challenges.

Risk 2: Intellectual Property and Legal Risks

AI introduces a complex web of legal and Intellectual Property (IP) challenges. Traditionally, when individuals or organisations commit errors or violate rules, they are held accountable under the law. However, this accountability becomes ambiguous in the case of AI. Questions arise about who is liable for AI-generated mistakes, and these uncertainties extend to IP issues, data privacy, bias, and ethical concerns.

A. Challenges in liability and accountability

AI systems often operate without clear accountability structures. If an AI model produces an error—such as a biased hiring decision or a fabricated medical diagnosis—pinpointing responsibility is challenging. Key questions include:

- **Who is at fault? Is it the developer, the user, or the AI system itself?**
- **How do we trace the source of the error?** Errors, particularly AI hallucinations, are often difficult to attribute due to the complex, non-transparent nature of AI systems.

Example: Self-driven cars In 2018, an **Uber** self-driving car killed a pedestrian in Arizona. Investigations revealed a combination of system flaws and human oversight failures, but no clear accountability was established. This case highlights the legal ambiguity surrounding AI-enabled systems. [22]

B. Intellectual property concerns

AI systems often rely on pre-existing IP, such as datasets, music, art, and software, raising significant questions about ownership:

1. Data models and copyright

AI models trained on copyrighted material blur the lines of IP ownership. For example, AI-generated artworks or music may borrow elements from copyrighted works, leaving creators without recognition or compensation.
Example: **Getty Images** filed a lawsuit against **Stability AI,** alleging that the AI used copyrighted images to train its model without permission. The company claimed its photos were scraped and used to generate AI outputs, violating copyright law. [23]

2. Disintermediation:

AI bypasses traditional pathways of content usage. For example, when a user searches on Google, the search engine typically credits the source. However, AI-generated responses may summarise or repurpose content without proper attribution.

C. Legal framework gaps

The rapid development of AI has outpaced the evolution of legal frameworks, leaving many areas unregulated:

1. **Intellectual property rights:** Current copyright laws often fail to address AI-specific issues, such as ownership of AI-generated content or liability for AI-created IP infringements.
2. **Data privacy and security:** AI systems frequently process vast amounts of personal data, increasing risks of misuse or data breaches.
   Example: **ChatGPT** Bans: Companies like **Apple, JPMorgan Chase, Citigroup, and Wells Fargo** have banned the use of AI tools like ChatGPT due to concerns over data leakage, security, and liability. [24]

In India's burgeoning EdTech sector, biased AI algorithms might inadvertently harm students' prospects, leading to lawsuits and loss of public trust.

D. Shadow IT and liability risks

AI tools are often adopted informally by employees or departments without proper oversight, a phenomenon known as 'shadow IT'. This creates a legal and liability nightmare, as unauthorised use of AI tools can lead to breaches of compliance and security policies.

Risk 3: Privacy Risks

As AI technology advances, it brings with it a heightened risk to individual and organisational privacy. AI's ability to collect, analyse, and leverage vast amounts of personal data has sparked serious concerns about data security and privacy. These risks necessitate a shift in focus from traditional privacy protection methods, such as anonymisation, to more advanced techniques like data encryption and differential privacy.

Key privacy risks in AI

1. **Massive data collection:** AI systems often rely on large datasets containing sensitive personal information, such as financial records, health data, and online behaviour. Without proper safeguards, this data becomes vulnerable to misuse, breaches, or unauthorised access.
2. **Lack of transparency:** Many AI systems operate as 'black boxes', where users cannot easily discern how their data is processed or used. This lack of transparency can lead to privacy violations, as users are unaware of how their information is being leveraged.
3. **Potential for misuse:** AI's capacity to analyse and predict user behaviour can lead to invasive practices, such as targeted surveillance, manipulation, or discrimination.

Example: **Facebook-Cambridge Analytica** scandal: In 2018, Cambridge Analytica improperly accessed data from millions of Facebook users to influence elections through targeted political ads. This incident highlighted the risks of AI-driven data misuse and the need for stricter privacy regulations. [25]

The call for global regulation

Both McKinsey and Microsoft stress the importance of a unified global framework to address privacy risks in AI:

1. **McKinsey** advocates for coherent regulatory collaboration between governments and organisations, emphasising that privacy protection should be a cornerstone of AI development. [2]
2. **Microsoft** calls for collective global efforts to design and implement privacy and ethical AI policies, ensuring safety and trust in AI systems worldwide. [2]

Addressing privacy risks in AI requires a collective and proactive approach that involves businesses, governments, and stakeholders. By adopting advanced privacy techniques, adhering to strict regulations, and fostering global collaboration, organisations can mitigate AI's privacy challenges while maintaining trust in the digital age.

Risk 4: Bias and Discrimination (Lack of Transparency)

AI systems have the potential to easily maintain the societal biases found in their training data. This can lead to biased decision-making, discrimination, and unfair treatment of certain groups. [9]

AI systems often operate non-transparently, making it challenging to understand how they make several decisions. This lack of transparency can lead to distrust among the users and stakeholders. To address this, businesses should prioritise transparency by designing AI models and algorithms that provide insights into their decision-making processes.

1. **Opaque decision-making:** AI systems often rely on complex algorithms and massive datasets to make decisions. However, the process by which these decisions are reached is frequently hidden from users. This opacity prevents stakeholders from verifying the accuracy or fairness of the outcomes.
2. **Algorithmic bias:** When the data used to train AI systems contains biases, the results may reinforce or even amplify these biases. Without transparency, it is challenging to identify or address these issues.

Example: **Amazon's AI Recruiting Tool:** In 2018, Amazon developed an AI recruiting tool that was later found to discriminate against women. The algorithm had been trained on historical hiring data, which reflected past biases favouring male candidates. Because the decision-making process was opaque, it took time to uncover and address the bias. [26]

Risk 5: Cybersecurity Risks

AI, while transformative and efficient, introduces significant cybersecurity challenges. The advanced capabilities of AI systems make them not only valuable assets but also prime targets for malicious actors. despite their efficiency, AI systems, are exposed to significant vulnerabilities and are susceptible to hacking, cyberattacks, and security breaches. Malicious activities can exploit AI systems and create more dangerous cyberattacks, posing a significant threat to businesses.

Adopting AI across various lines of business can introduce a range of cyber threats, as AI systems process large amounts of sensitive data, make autonomous decisions, and integrate deeply into critical infrastructures. Here's a breakdown of potential cyber threats with examples, particularly in the Indian context:

a. **Data breaches and privacy violations**
   AI systems rely on vast amounts of sensitive data, including personal, financial, and operational information. If these systems are compromised, attackers can exploit or expose confidential data.

   Example: **Aadhaar Data Breach:** India's Aadhaar system faced massive data leaks, exposing sensitive personal information. While not AI-specific, integrating AI into such systems could amplify risks, as it processes and stores even larger datasets. [27]

b. **Adversarial attacks**
   Hackers can exploit AI models by feeding deceptive data, leading to incorrect predictions or decisions.

   Example: **Facial recognition manipulation:** AI-powered surveillance systems in India, such as those in airports (e.g., Digi Yatra), could be tricked with adversarial inputs, allowing unauthorised individuals to bypass security. [28]

c. **AI model theft**
AI models are valuable intellectual property (IP). Cybercriminals may steal or reverse-engineer these models for competitive or financial gain.

Example: AI models used by e-commerce giants like **Flipkart or Myntra** could be targeted, enabling attackers or competitors to replicate proprietary recommendation algorithms. [29]

d. **Automated cyberattacks**
Attackers can leverage AI to create sophisticated, adaptive, and automated cyberattacks, such as phishing campaigns.

Example: During the **COVID-19** pandemic, phishing attacks surged in India. AI could enhance these attacks, making them highly personalised and increasing their success rates. [30]

e. **Deepfakes and synthetic identity fraud**
AI-generated deepfakes can be used for misinformation, fraud, or impersonation, undermining trust and security.

Example: **Political deepfakes in India:** AI-generated videos have been used during elections to spread propaganda.

f. **Bias exploitation in AI models**
AI models trained on biased data can lead to discriminatory decisions, which attackers could exploit to undermine trust or create legal liabilities.

Example: In India, AI-based credit scoring systems adopted by **NBFCs** and banks could inadvertently discriminate against specific groups, raising ethical and legal concerns. [31]

g. **AI Supply Chain Attacks**
AI systems depend on third-party APIs, datasets, and libraries. If these are compromised, vulnerabilities could cascade across multiple organisations. Example: An attack on an Indian AI vendor serving banks, retailers, and healthcare providers could lead to widespread disruptions across industries. [32]

g. **AI supply chain attacks**
AI systems depend on third-party APIs, datasets, and libraries. If these are compromised, vulnerabilities could cascade across multiple organisations.

Example: An attack on an **Indian AI vendor serving banks,** retailers, and healthcare providers could lead to widespread disruptions across industries. [32]

h. **Ransomware and AI-controlled malware**
Attackers could use AI to design more sophisticated ransomware or malware-targeting AI systems.

Example: In 2021, **AIIMS Delhi** experienced a ransomware attack. Future AI-driven attacks could cripple critical infrastructure like hospitals, especially with AI-integrated diagnostic systems. [33]

i. **Operational disruptions via AI manipulation**
Manipulating AI systems in critical sectors such as manufacturing, logistics, or energy can disrupt operations and create economic chaos.

Example: AI-powered logistics systems used by companies like **Delhivery** could be targeted, causing widespread supply chain disruptions, especially during peak seasons. [34]

Risk 6: Dependence on AI

Excessive reliance on AI can lead to a decline in human skills, as individuals may become less engaged in problem-solving and decision-making. For instance, researchers have highlighted the issue of "model collapse", where generative AI models that are trained on synthetic data may produce lower-quality results because they simply prioritise common word choices over creative alternatives.

This dependency risks creating a workforce that lacks adaptability and resilience when AI systems fail or encounter limitations.

Businesses must train their employees to work alongside AI to avoid the potential risks of AI. In addition to this, the use of diverse training data and regularisation techniques can also help in mitigating these challenges associated with model collapse.

Real-life concerns

1. **Education:** Over-reliance on AI tools like ChatGPT for academic purposes might discourage students from developing critical thinking and research skills. A study highlighted that students using AI for essay writing often struggled with original thought. [35]
2. **Business decision-making:** Organisations that rely entirely on AI for strategic decisions might fail to consider human-driven insights or unquantifiable factors such as cultural nuances, resulting in suboptimal outcomes.

Risk 7: Job Loss and Unintended Consequences

AI has significantly transformed various industries, enhancing efficiency and productivity. However, its rapid integration has introduced challenges, notably job displacement and unintended consequences arising from errors and omissions. AI-driven automation has the potential to displace jobs across various industries, with lower-skilled workers being the top-most targets.

Understanding these challenges is crucial for developing strategies that balance technological advancement with societal well-being. Due to their complexity, AI systems may exhibit unexpected behaviours or make decisions with unforeseen consequences.

a. **Job displacement due to AI-driven automation**
AI-driven automation has the potential to displace jobs across various industries, with lower-skilled workers being the top-most targets. For each one-unit increase in AI, the employment share of lower-skilled workers decreases by 0.001% due to the replacement effect. [42]

b. **Unintended consequences: errors and omissions in AI systems**
AI systems, due to their complexity, may exhibit unexpected behaviours or make decisions with unforeseen consequences. Rigorous testing, validation, and continuous monitoring processes are essential to identify and address these issues before they escalate and cause harm. [11]

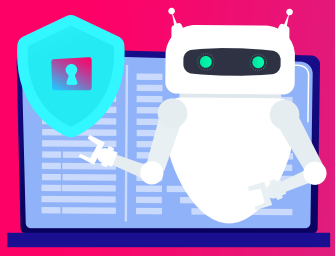
Risk 8: Misinformation and Manipulation

AI-generated content like deepfakes poses a significant risk by contributing to spreading false information and manipulating public opinion. Understanding these challenges is crucial for developing strategies that balance technological advancement with societal well-being.

AI technologies, particularly deep learning models, have the capability to generate realistic images, videos, and audio, making it increasingly difficult to distinguish between authentic and fabricated content. This capability has been exploited to create deepfakes—manipulated media that can deceive audiences and spread misinformation.

Real-life example

Corporate disinformation: Companies have become targets of AI-driven disinformation campaigns. False claims about products or services can spread rapidly, damaging reputations and financial standing. For example, a fabricated video alleging a food company's involvement in unethical practices can lead to public backlash and financial losses. [36]



4. Insurance Coverage

The integration of AI into business operations introduces unique risks, prompting questions about insurance coverage for AI-related losses in India. Here's an overview of the current landscape:

a. Cyber insurance policies:
In India, cyber insurance policies are designed to cover losses from cyber incidents, including data breaches, ransomware attacks, and business interruptions caused by cyber events. While these policies address certain risks associated with AI, such as data breaches resulting from AI system failures, they may not comprehensively cover all AI-related perils.

b. Emerging AI-specific insurance products:
Globally, there is a growing recognition of the need for AI-specific insurance products. For instance, **AXA XL** has introduced new cyber insurance coverage to manage emerging generative AI risks, addressing issues like data poisoning and usage rights infringement. However, such specialised products are yet to be introduced in the Indian market. [37]

c. Coverage gaps and challenges:
AI-related risks can span various domains, including product liability, professional liability, and intellectual property infringements. Traditional insurance policies may not explicitly cover these risks, leading to potential coverage gaps. For example, if an AI-powered product causes harm due to a malfunction, it might not be clear whether product liability or cyber insurance would respond. [38]

d. Need for policy evolution:
As AI technologies evolve, there is a pressing need for the insurance industry in India to develop tailored products that address the specific risks associated with AI. This includes understanding the unique challenges posed by AI and creating policies that offer comprehensive coverage for AI-related perils. [39]

e. Property insurance:

- **Physical damage caused by AI:** If AI systems cause physical damage (e.g., a malfunctioning robot damages equipment), the damage may be covered if it results from an insured peril like equipment breakdown. Many policies exclude damage caused by programming errors or cyber incidents.
- **Cyber-related incidents:** If AI is hacked or manipulated, resulting in physical damage, most property policies exclude damages caused by cyberattacks unless cyber insurance is in place. Standalone cyber insurance policies may address losses caused by AI-driven cyber events.

f. Motor Insurance:

Accidents caused by AI (self-driving features)

i. Covered under standard policies:

Most motor insurance policies cover damages caused by accidents, regardless of whether the vehicle was being driven manually or autonomously. The insurer usually holds the vehicle owner liable for the damages.

ii. Potential manufacturer liability:

If the accident is proven to have resulted from a defect or malfunction in the AI system (e.g., failure of autonomous braking), the insurer may subrogate the claim and seek recovery from the manufacturer or software provider.

iii. **Cyber risks and hacking**

Exclusions in standard policies:

Losses caused by hacking or unauthorised access to AI systems are typically excluded from motor insurance. For example:

- A hacked autonomous vehicle causing an accident
- Data breaches involving vehicle systems

iv. **AI system errors or malfunctions**

Grey Area:

Errors in AI decision-making (e.g. misjudgement of road conditions) are generally treated as mechanical or system malfunctions. Some policies may exclude such events under "mechanical breakdown" exclusions, leaving coverage unclear.

v. **Liability shifts with autonomous vehicles**

- **Shift to product liability:** raditional motor insurance models may shift, with manufacturers and software developers bearing more liability for AI-related incidents. Insurance could evolve into product liability coverage for manufacturers rather than personal motor policies.
- **Government and regulatory influence:** Regulatory frameworks (e.g., UK's Automated and Electric Vehicles Act) are influencing how insurers address liability for AI-driven accidents.

vi. **Covered under standard policies:**

Theft of the vehicle itself is typically covered. However, losses caused by misuse of AI systems (e.g., theft enabled by exploiting AI vulnerabilities) may not be explicitly covered unless specified in the policy.

Excerpts from the industry experts

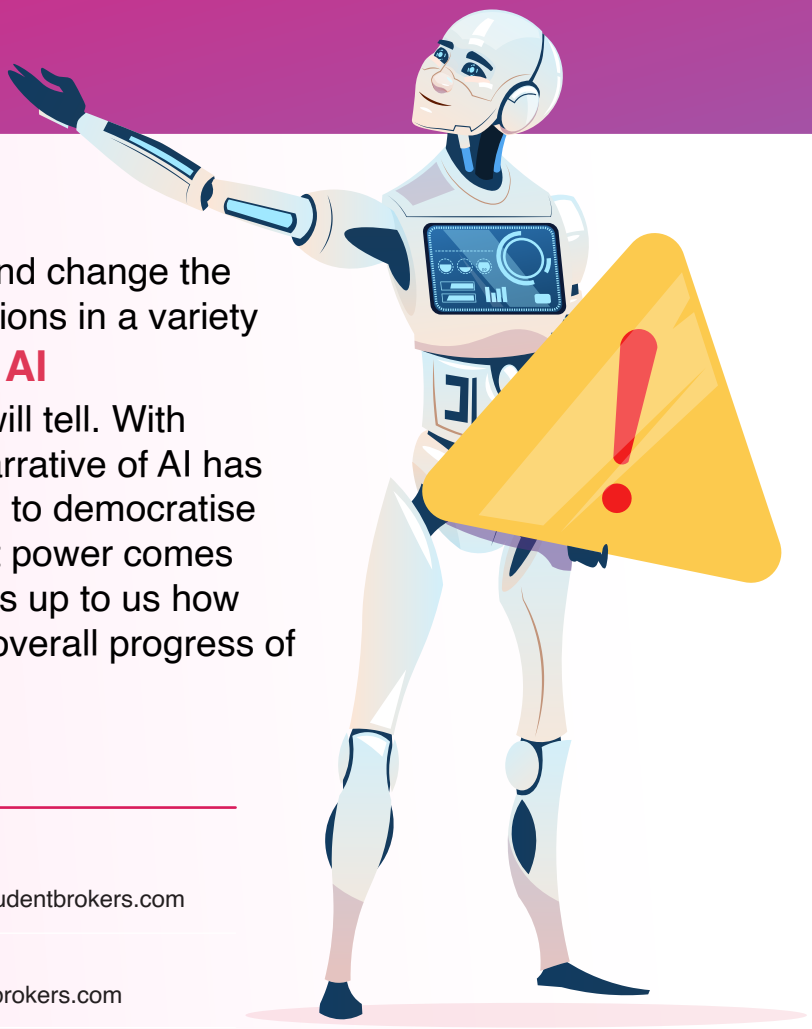
"We utilise AI technologies to enhance the accuracy and efficiency of identifying potential risks across various domains, including financial, legal, and operational sectors. By implementing sophisticated algorithms and machine learning models, Ankura can analyse vast data sets to detect anomalies and predict emerging risks before they manifest."

Amol Pitale
Managing Director, Ankura Consulting Group, LLC

"AI is undeniably transforming cybersecurity by enabling proactive, efficient, and scalable solutions. While its benefits far outweigh its challenges, addressing concerns like adversarial AI, false positives, and privacy risks is critical. A balanced approach that combines AI capabilities with human expertise is essential to maximise its potential and build a robust cybersecurity framework."

Umesh Mehta
Independent Director, 3i Infotech Ltd.

Conclusion



AI will be a game changer and change the way in which humanity functions in a variety of ways. **"AI for ALL and AI Everywhere"-** only time will tell. With DeepSeek coming in, the narrative of AI has further changed, as it claims to democratise this invention. But with great power comes greater responsibility and it is up to us how we use AI capability for the overall progress of mankind.

Authored by:

Neha Anand
Head of Cyber Insurance I neha.anand@prudentbrokers.com

Vivek Bhajipale
Cyber Specialist I vivek.bhajipale@prudentbrokers.com

Tanmay Rajesh Tanawade
Manager Liability Placement I tanmay.tanawade@prudentbrokers.com

Sources

1. Harnessing Tech Trends:Integrating AI into Everyday Business Operations | LinkedIn
2. 5 AI Risks for Organizations. How Business Leaders Can Overcome Them?
3. https://m.economictimes.com/tech/technology/ai-adoption-in-key-indian-sectors-touches-48-in-fy24/articleshow/110060391.cms
4. https://www.induqin.com/post/rapid-adoption-of-artificial-intelligence-across-india-s-industries
5. https://medial.app/news/ai-adoption-in-key-indian-sectors-touches-48percent-in-fy24-17c1fb5e86e60
6. https://www.cio.inc/fmcg-industry-drives-innovation-ai-adoption-a-25719
7. https://medibulletin.com/healthcare-industry-fastest-in-adopting-artificial-intelligence-show-new-data/
8. https://advisorsindia.in/ai-adoption-in-key-indian-sectors-touches-48-in-fy24/
9. Navigating AI Risks: Safeguarding Businesses from the Impact of AI
10. PayPal's AI Security Enhancements Explained
11. The 15 Biggest Risks Of Artificial Intelligence
12. Revolutionizing Manufacturing: Navigating the Artificial Intelligence Landscape for Efficiency, Ethics, and Growth by Gunter Beitinger on Siemens Blog
13. Generative Design AI Software
14. Artificial Intelligence In Boeing Flight Manufacturing – Laminar Sim
15. The Amazing Ways Chinese Tech Giant Alibaba Uses Generative Artificial Intelligence
16. The State of AI Infrastructure at Scale 2024
17. Top 21 AI use cases in eCommerce (the rise of AI in eCommerce) | Instant
18. AI in Fashion: Transforming Indian Industry - Technopak Advisors
19. From FreshToHome, Nykaa, Flipkart; How AI has changed the dynamics in the retail industry - Digital Transformation News | The Financial Express
20. a. https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020#:~:text=Thanks%20in%20part%20to%20the%20growth%20of,State%20of%20Phishing%202024"%20report%20from%20SlashNext.
    b. https://www.cobalt.io/blog/top-40-ai-cybersecurity-statistics
    c. https://secureframe.com/blog/generative-ai-cybersecurity#:~:text=In%20a%20report%20by%20Deep%20Instinct%2C%2075%,rise%20to%20bad%20actors%20using%20generative%20AI
    d. https://www.nyu.edu/life/information-technology/safe-computing/protect-against-cybercrime/ai-assisted-cyberattacks-and-scams.html#:~:text=Attackers%20can%20leverage%20AI%20to,to%20detect%20and%20defeat%20threats.
    e. https://www.helpnetsecurity.com/2024/04/25/cybersecurity-ai-stats/#:~:text=AI%20tools%20put%20companies%20at%20risk%20of,had%20sensitive%20data%20breached%2C%20leaked%2C%20or%20exposed.
    f. https://abnormalsecurity.com/glossary/ai-enabled-cyberattacks#:~:text=What%20is%20an%20AI%2DPowered,and%20learn%20from%20their%20targets.
    g. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/#:~:text=AI%2Ddriven%20phishing%20attacks%20use,access%20a%20system%20or%20device
21. deepmind.google/research
22. National Transportation Safety Board
23. Reuters, January 2023
24. Bloomberg, May 2023
25. The Guardian, 2018
26. Reuters, 2018
27. Quartz India, 2018
28. Business Standard, 2023
29. The Economic Times, 2021
30. McAfee, 2020
31. Livemint, 2022
32. Financial Express, 2023
33. Hindustan Times, 2021
34. Business Today, 2022
35. The Guardian, 2023
36. Financial Times
37. AXA XL unveils new cyber insurance coverage to manage emerging Gen AI risks, ET CIO SEA
38. AI and Insurance: Managing Risks in the Business World of Tomorrow | Herbert Smith Freehills | Global law firm
39. Insurance coverage issues, artificial intelligence and deepfakes | Reuters
40. Publications - Amazon Science
41. IBM Watson
42. PMC

PRUDENT
THE FUTURE OF INSURANCE

WWW.PRUDENTBROKERS.COM

PRUDENT INSURANCE BROKERS PVT. LTD. (Composite Broker)

Certificate of Registration IRDAI No. 291 & IFSCA No. 017 (Validity: 18th February 2023 to 17th February 2026)

Registered office at 1st Floor, Tower B, Peninsula Business park, G.K. Marg, Lower Parel, Mumbai – 400013, Maharashtra
Tel : +91 22 3306 6000 I CIN No.: U70100MH1982PTC027681

PIBL_Advt24-25_111