WEBINAR

Navigating the Future: Gen AI and Mitigating Risks for Technology Leaders

MODERATED BY
EMILY HEMINGWAY
EXECUTIVE DIRECTOR
TECH STL

ANDREW MONTGOMERY
VP OF STRATEGY
OBJECT COMPUTING

DR. YAQI CHEN
DIR OF AI / ML
OBJECT COMPUTING

BRANDON LYNCH
SECURITY ENGINEER
OBJECT COMPUTING

WEDNESDAY, JAN. 17 | 10AM CST

Please type your questions into the Chat. We will try to answer all of them near the end of the webinar.

This webinar is being recorded.

We will send an email with the presentation after the webinar.

Presenters

Emily Hemingway
Exec. Director of Tech STL

Andy Montgomery
VP of Strategy

Dr. Yaqi Chen
Director of AI / ML

Brandon Lynch
Security Engineer

© 2024 Object Computing, Inc. All rights reserved.

Agenda

- Who is Object Computing?
- The State of AI
- Addressing Risks and Mitigation Strategies
- Q & A

© 2024 Object Computing, Inc. All rights reserved.

Introduction

For 30 years, we've helped clients discover new business frontiers with breakthrough technologies while delivering measurable business outcomes.

We specialize in software engineering, AI, machine learning, DLT/blockchain, and connected, scalable solutions.

We work with organizations like US Intelligence Agencies, mission-critical operations like NASA, industry disruptors like Bloomberg and transportation innovators like Class 1 Railroads.

© 2024 Object Computing, Inc. All rights reserved.

Object Computing Offerings

APPLICATION DEVELOPMENT

WE CAN CUSTOM-BUILD YOUR APP

APPLICATION MODERNIZATION

WE CAN FUTURE-PROOF LEGACY APPS

AI CONSULTING AND DATA INSIGHTS

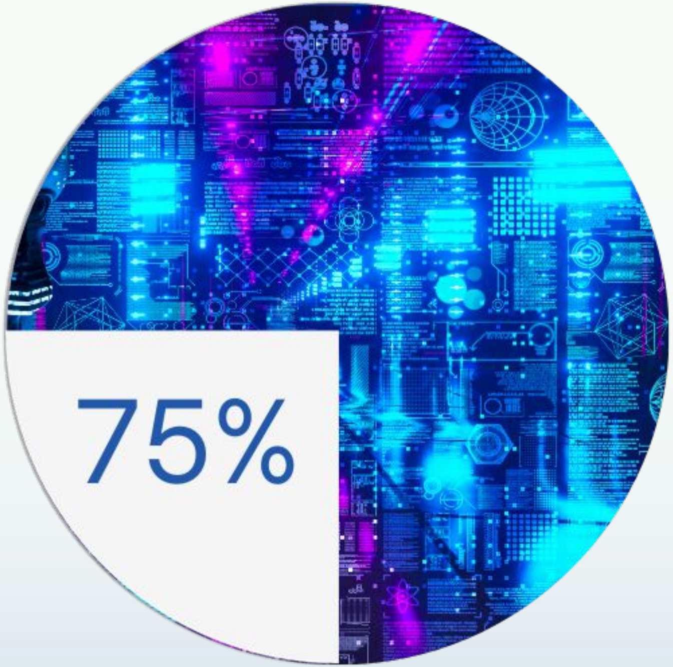
WE EMPOWER SMARTER DECISION-MAKING

EMBEDDED ENGINEERING

WE CAN BUILD OR STRENGTHEN YOUR TEAM

© 2024 Object Computing, Inc. All rights reserved.

Unlocking Value Across Industries

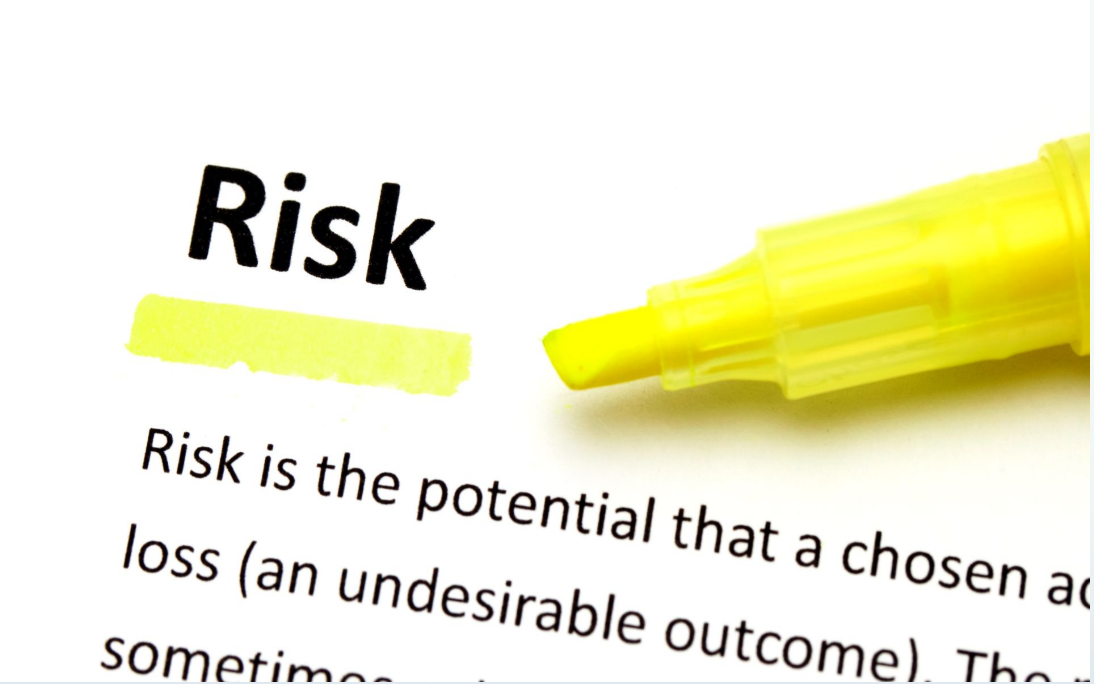


75% of the value generated by Gen AI will be in these 4 disciplines

- Customer Operations
- Sales and Marketing
- Software Engineering
- Research and Development

© 2024 Object Computing, Inc. All rights reserved.

Addressing Risks and Challenges



Risk

Risk is the potential that a chosen ac
loss (an undesirable outcome). The
sometim

Recent research by McKinsey

- 33% of respondents' organizations are using Gen AI regularly
- 40% intend to boost AI investment due to Gen AI advancements
- Less than 50% indicate their organizations are actively mitigating the risk they find most pertinent

© 2024 Object Computing, Inc. All rights reserved.

Gen AI Risks

Ineffective Queries and Hallucinations

Data Security and Privacy

Model Security and Explainability

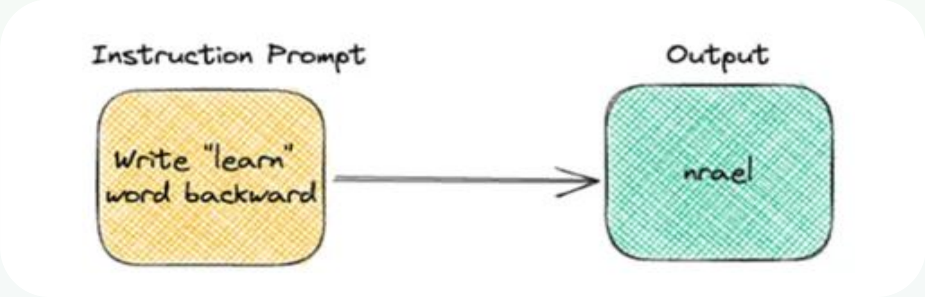
Regulatory Compliance

© 2024 Object Computing, Inc. All rights reserved.

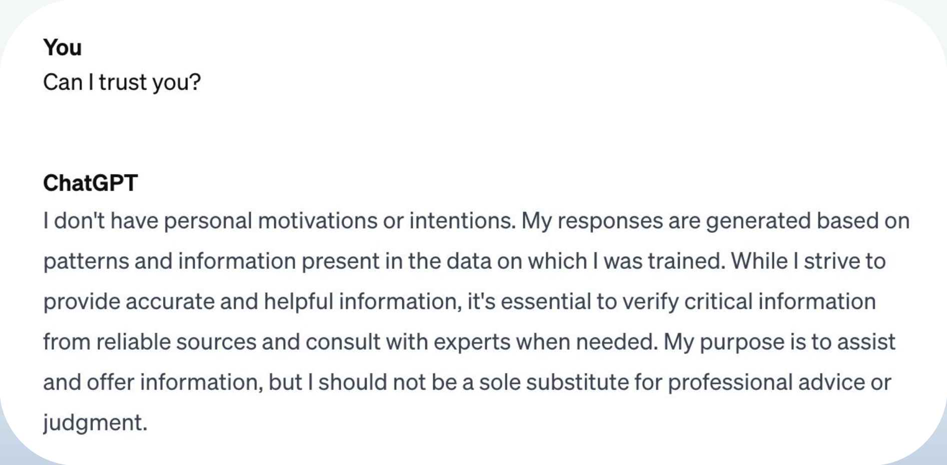
RISK:

Ineffective Queries and Hallucinations

Ineffective Queries or Misuse of Prompt Engineering



Hallucinations: Gen AI app provides seemingly factual information but does not answer the question correctly



You

Can I trust you?

ChatGPT

I don't have personal motivations or intentions. My responses are generated based on patterns and information present in the data on which I was trained. While I strive to provide accurate and helpful information, it's essential to verify critical information from reliable sources and consult with experts when needed. My purpose is to assist and offer information, but I should not be a sole substitute for professional advice or judgment.

© 2024 Object Computing, Inc. All rights reserved.

MITIGATION STRATEGY:

Ineffective Queries and Hallucinations

1 Adopt Best Practices: providing context, using descriptive languages, taking an interactive approach, etc.

© 2024 Object Computing, Inc. All rights reserved.

MITIGATION STRATEGY:

Ineffective Queries and Hallucinations

1. Adopt Best Practices: providing context, using descriptive languages, taking an interactive approach, etc.
2. Keep human-in-the-loop: institute new and relevant quality checks and verification process

© 2024 Object Computing, Inc. All rights reserved.

MITIGATION STRATEGY:

Ineffective Queries and Hallucinations

1. Adopt Best Practices: providing context, using descriptive languages, taking an interactive approach, etc.
2. Keep human-in-the-loop: institute new and relevant quality checks and verification process
3. Perform different levels of quality checks on AI-assisted tools based on risk tolerance

© 2024 Object Computing, Inc. All rights reserved.

MITIGATION STRATEGY:

Ineffective Queries and Hallucinations

1. Adopt Best Practices: providing context, using descriptive languages, taking an interactive approach, etc.
2. Keep human-in-the-loop: institute new and relevant quality checks and verification process
3. Perform different levels of quality checks on AI-assisted tools based on risk tolerance
4. Factual verification by Implementing verification process to cite data sources or to provide factual contexts

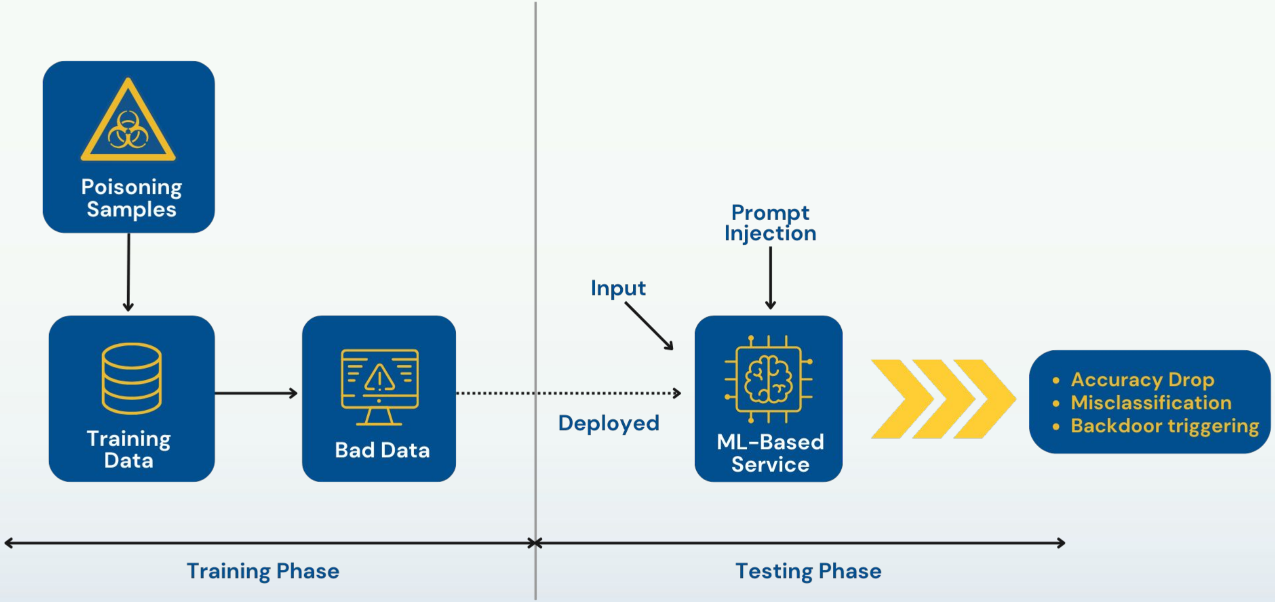
© 2024 Object Computing, Inc. All rights reserved.

RISK:
Model Security and Explainability

Model Poisoning

Backdoor Attacks

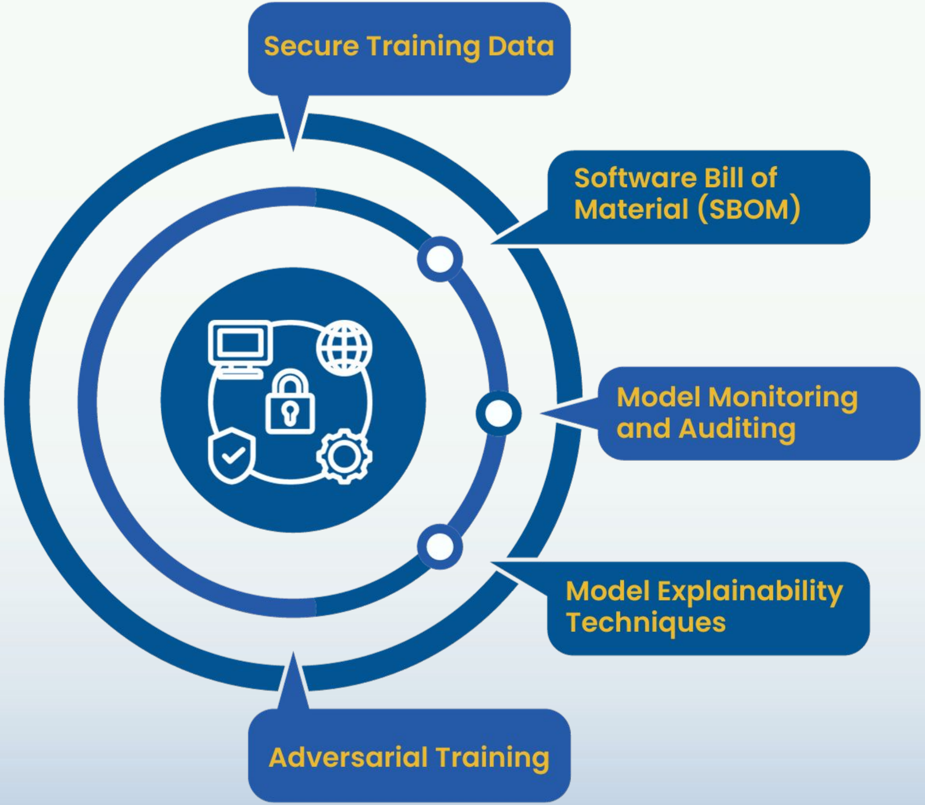
Model Evasion Attacks & Prompt Injection



© 2024 Object Computing, Inc. All rights reserved.

MITIGATION STRATEGY:

Model Security and Explainability



Secure Training Data

Software Bill of Material (SBOM)

Model Monitoring and Auditing

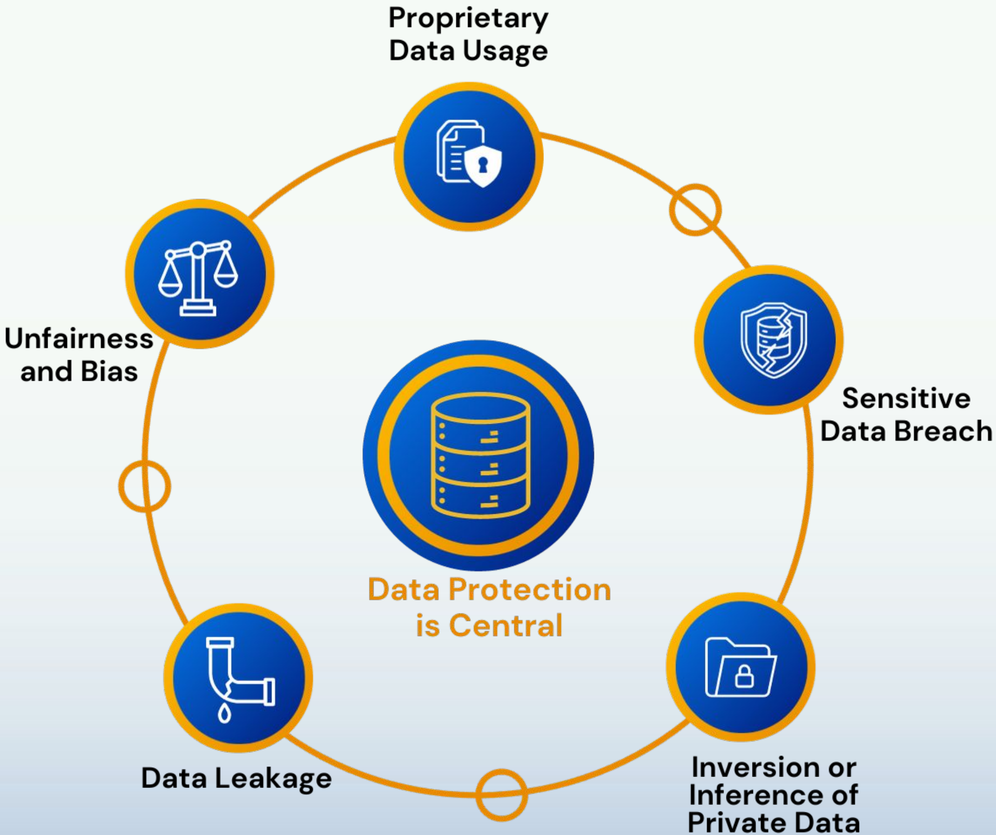
Model Explainability Techniques

Adversarial Training

© 2024 Object Computing, Inc. All rights reserved.

RISK:

Data Security and Privacy



Proprietary Data Usage

Sensitive Data Breach

Inversion or Inference of Private Data

Data Leakage

Unfairness and Bias

Data Protection is Central

© 2024 Object Computing, Inc. All rights reserved.

MITIGATION STRATEGY:

Data Security and Privacy

- Data Minimization
- Data Anonymization
- Data Encryption
- Access Control

© 2024 Object Computing, Inc. All rights reserved.

RISK:

Meeting Regulatory Compliance

Regulatory Uncertainty

Regulatory Reporting and Auditing

International Compliance

Source:
CISA

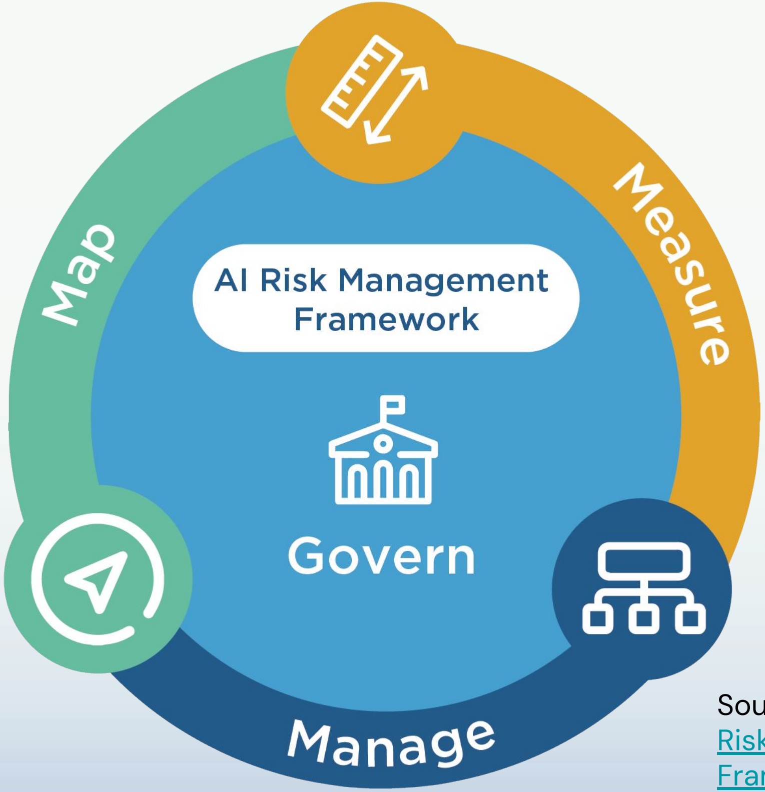
© 2024 Object Computing, Inc. All rights reserved.

MITIGATION STRATEGY:

Regulatory Compliance

New Regulations

Evolving Frameworks



Source: [NIST AI Risk Management Framework]

© 2024 Object Computing, Inc. All rights reserved.

Gen AI Risks and Mitigation Strategies

Ineffective Queries and Hallucinations

Mitigation Strategies:

- Adopt Best Practices In Query Configuration
- Human in the Loop
- Quality Checks
- Factual Verification

Data Security and Privacy

Mitigation Strategies:

- Data Minimization
- Data Anonymization
- Data Encryption
- Model Security

Model Security and Explainability

Mitigation Strategies:

- Secure Training Data
- Model Validation and Testing
- Model Monitoring and Auditing
- Model Explainability Techniques
- Adversarial Training

Regulatory Compliance

Mitigation Strategies:

- Keep abreast of new regulations
- Stay aware of evolving frameworks

© 2024 Object Computing, Inc. All rights reserved.

RECOMMENDATION:

Implementing Mitigation Strategies

Defense-in-depth framework

Regular audits and assessments

Collaborate with trusted partners

Ask them to identify specific ways to get guidance immediately

- Amplify intelligence
- Accelerate insights
- Prescribe success

© 2024 Object Computing, Inc. All rights reserved.

Please type questions into the Chat.

We will answer them now.

OBJECT COMPUTING

YOUR OUTCOMES ENGINEERED

Matt Bremehr
Sales Director
Object Computing Inc.

BremehrM@objectcomputing.com

ObjectComputing.com