

Model

GPT-4



ChatGPT **PLUS**



GPT-4 currently has a cap of 25 messages every 3 hours.

Send a message.



ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT Mar 23 Version](#)

The LBMC logo is displayed in white, sans-serif capital letters within a solid blue rectangular box in the top-left corner of the image.

LBMC

The background of the slide is a photograph of a modern, multi-story office building with a glass facade. The building's glass reflects the sky and surrounding environment. The LBMC logo is also visible on the building's exterior. Bare trees are visible in the foreground and to the right of the building.

LBMC

Generative AI: Your New Secret Weapon or Insider Threat

APRIL 26, 2024

LBMC.COM

About the speaker

Chris Collins, Senior Manager

CISA 2010, CRISC 2016, CISSP 2016

CRISC Exam Result Notification

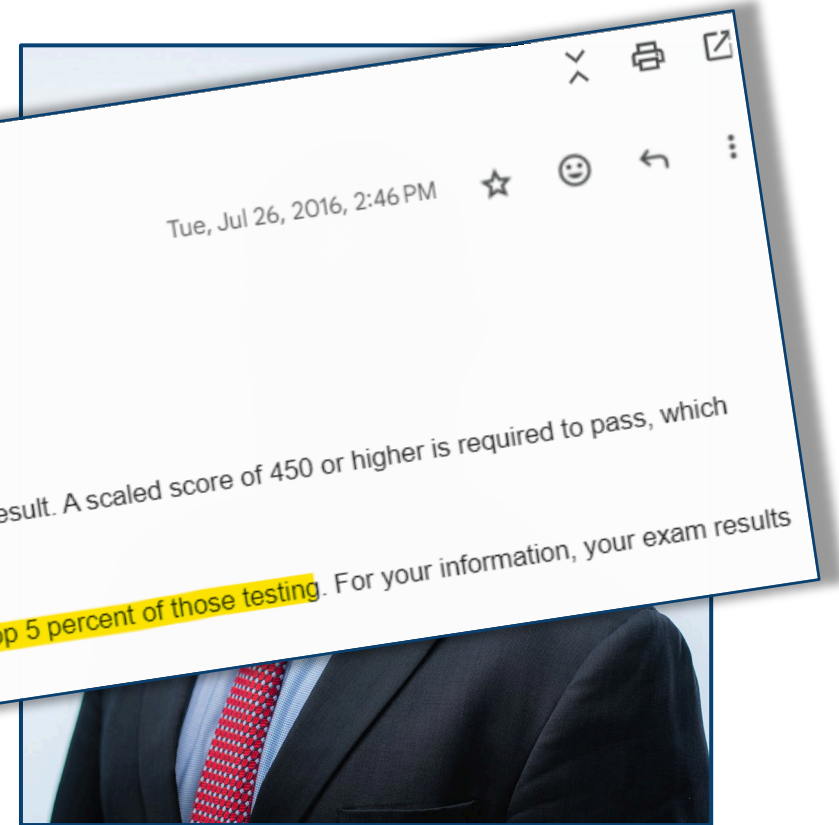
Exam <exam@isaca.org>
to me

Dear Christopher Collins:

RE: CRISC Exam Result Notification -- Exam ID: 16575639

At your request (per your exam registration authorization), this email is being sent to notify you of your June 2016 CRISC exam result. A scaled score of 450 or higher is required to pass, which represents the minimum consistent standard of knowledge as established by ISACA's CRISC Certification Working Group.

We are pleased to inform you that you successfully PASSED the exam with a total scaled score of 608. **Your score was in the top 5 percent of those testing.** For your information, your exam results by area are provided below.



About LBMC

- #1 Accounting and Business Consulting Firm in Tennessee
- #3 in the Southeast
- Top 40 Nationwide



Agenda

- What Is Generative AI?
- How Can We Use It?
- What Are The Risks?
- Where Do We Go From Here?
- 90-Day AI Strategy Plan

What Is Generative AI?

Generative AI is a type of artificial intelligence system capable of generating text, images, or other media in response to prompts.



ChatGPT

Tampa's bay glimmers,
Pirates sail through misty dreams,
Treasure bathed in light.



Large Language Models (LLMs)

2018	2019	2020	2021	2022	2023
BERT	XLNet	GPT-3	GPT-Neo	LaMDA	LLaMA
	GPT-2		GPT-J	GPT-NeoX	GPT-4
			Megatron-Turing NLG	Chinchilla	Cerebras-GPT
			Ernie 3.0 Titan	PaLM	Falcon
			Claude	OPT	BloombergGPT
			GLaM	TaLM 100B	PanGu-Σ
			Gopher	Minerva	OpenAssistant
				BLOOM	PaLM 2
				Galactica	
				AlexaTM	



ChatGPT



Copilot

Gemini

Time to Reach 1 Million Users

The Netflix logo, consisting of the word "NETFLIX" in a bold, red, sans-serif font.

3.5 Years



2 Years

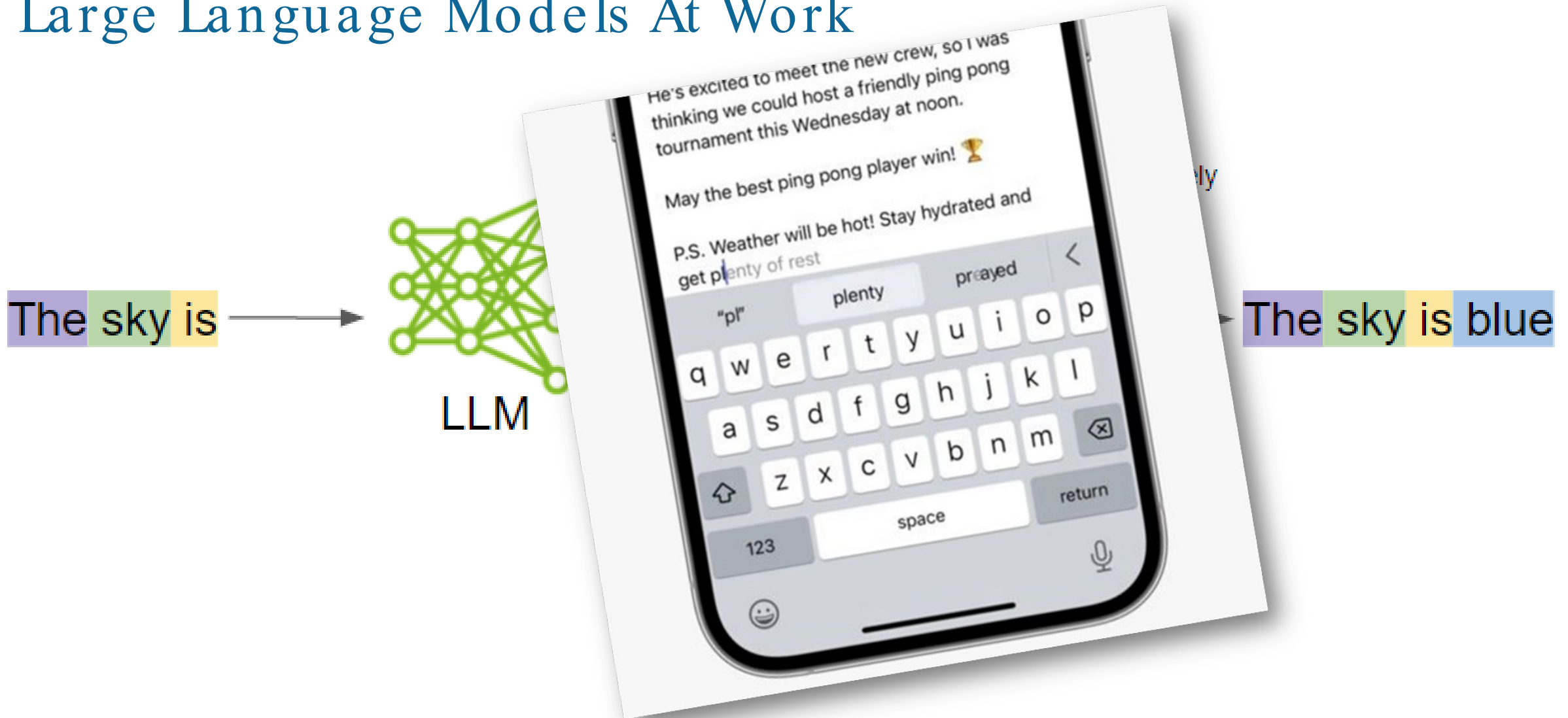


2.5 Months



5 Days

Large Language Models At Work



Think of language models like
ChatGPT as a “calculator for words”

-Simon Willison

Your New Secret Weapon
(How Can We Use It?)

Document Templates

- Policies
- Procedures
- Configuration Standards
- Incident Response Plans



System Configuration Guidance

- Logging
- Password Settings
- NTP
- Encryption



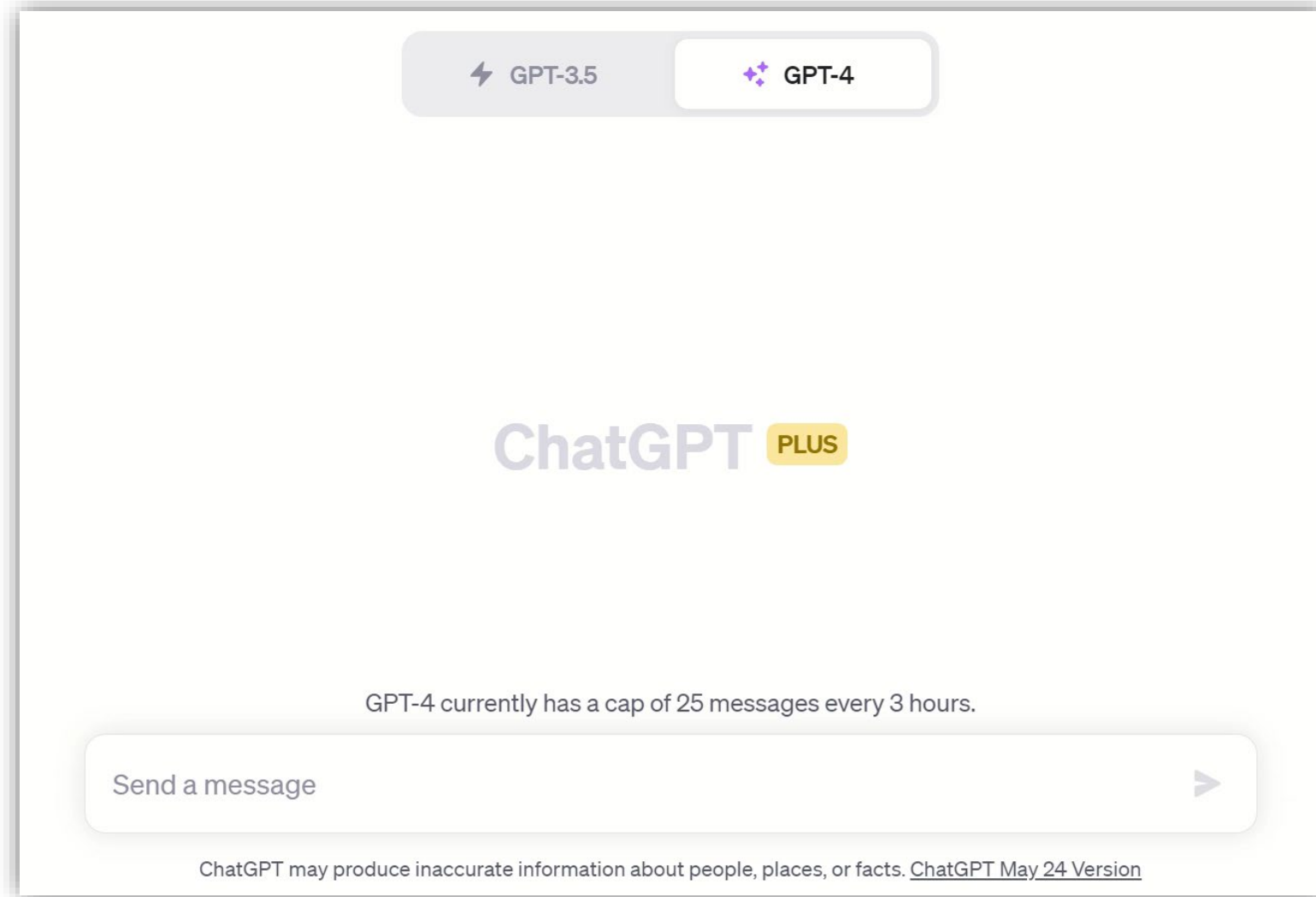
Scripts and Coding

- PowerShell
- Python
- HTML/CSS
- Shell Scripting (Bash)
- JavaScript
- C++
- COBOL



Process Facilitation

- Incident Response
Tabletop
- Scoping Exercise



Q&A With An AI

Microsoft Bing SEARCH CHAT

Kyle.Hinterb... Protected

PCI DSS 4.0 payment page scripts

What is the new INFI worksheet for PCI DSS compliance?

View other drafts

The INFI worksheet is a new tool that was released by the PCI Security Standards Council in June 2023. It is designed to help organizations identify and document areas needing improvement in their security posture. The worksheet is intended for use by Qualified Security Assessors (QSAs) during PCI DSS assessments, but it can also be used by organizations for self-assessment.

The INFI worksheet includes the following sections:

- **Summary:** This section provides a brief overview of the organization's security posture, including the number of PCI DSS requirements that are met, partially met, and not met.
- **Items Noted for Improvement:** This section lists specific areas where the organization's security posture can be improved. Each item includes a description of the issue, the impact of the issue, and the recommended remediation steps.
- **Root Cause Analysis:** This section provides an analysis of the root causes of the issues

accordance with PCI

KH

with PCI DSS v4.0:

never possible. Server-

rs.

the input validation and

ore acting on it.

lds like credit card

re render

Searching for: **limitations of FA**

Generating answers for you...

Your personal and company

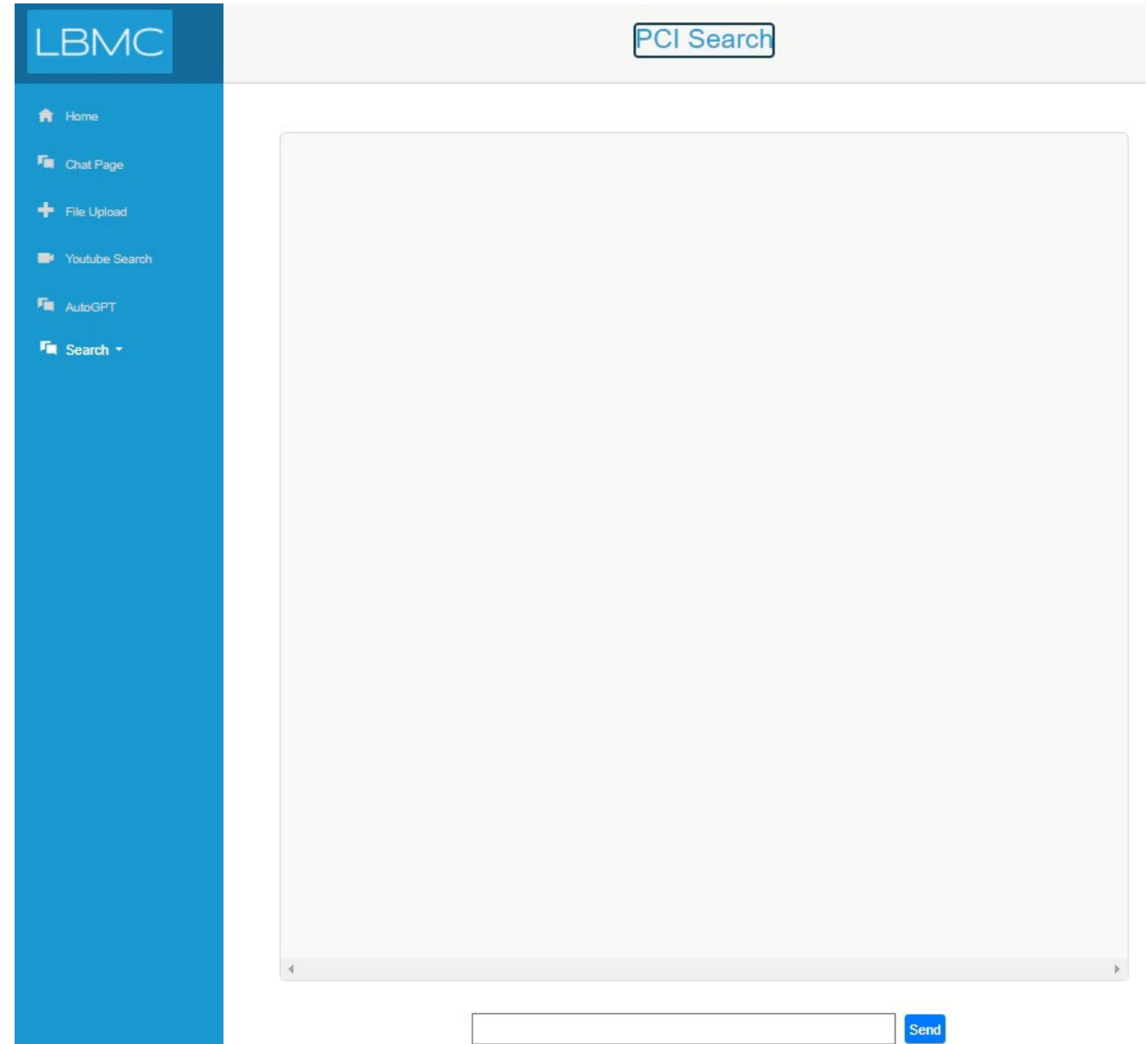
The FAIR (Factor Analysis of I

1. **Estimation:** FAIR does a gr².
2. **Taxonomy:** FAIR requires a too restrictive².
3. **Lack of Metrics:** Some use methodologies^{1 2}.
4. **Documentation:** FAIR is co of its methods³.
5. **Independence:** FAIR cannot improves risk assessment

Remember, no risk model is p

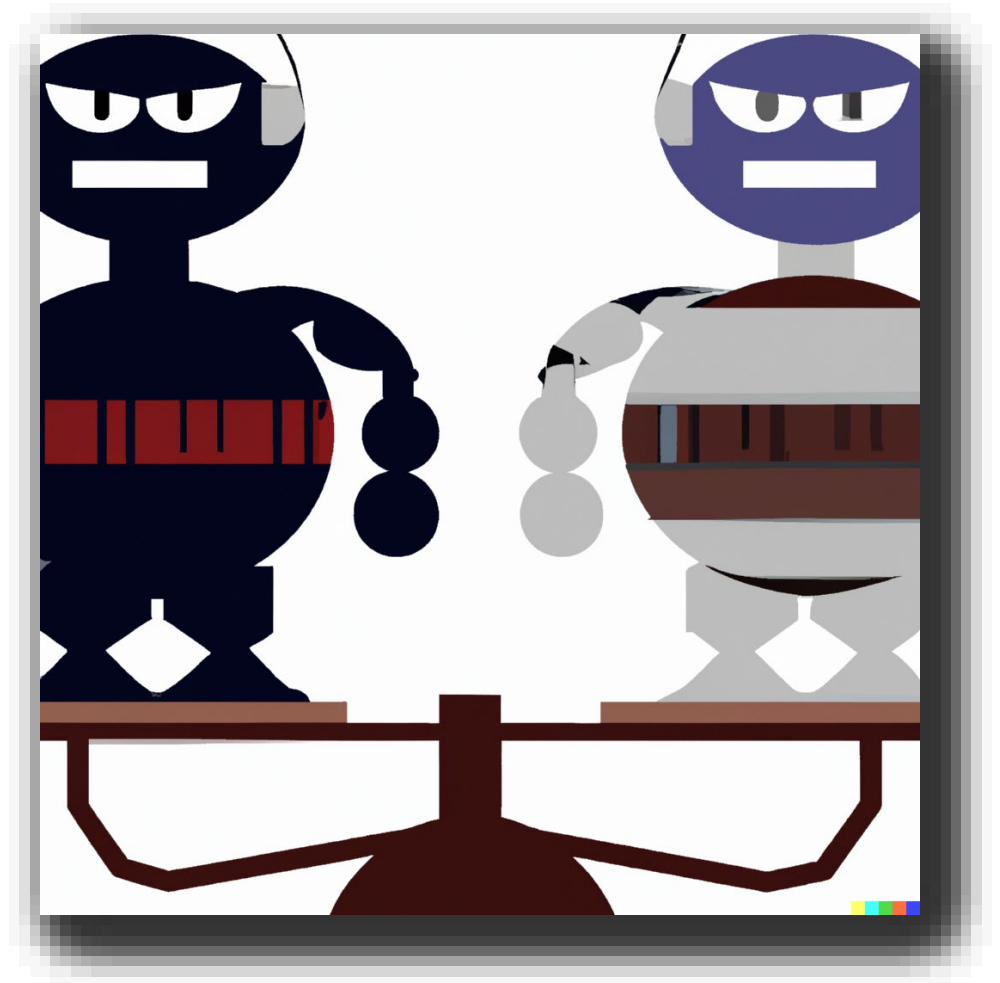
Private Generative AI Tools

- Contract Review
- Content Generation
- Technical Writing
- Risk Management
- Research & Development



AI-Prompt Engineering Best Practices

- Be Specific
- Provide Context
- Consider the AI's perspective
- Prompt Length
- Clear Language
- Instruction Prompts
- Try, Refine, Repeat
- Limit Bias
- Ethics



Insider Threats
(What Are The Risks?)

Unreliable Results

Best Practices

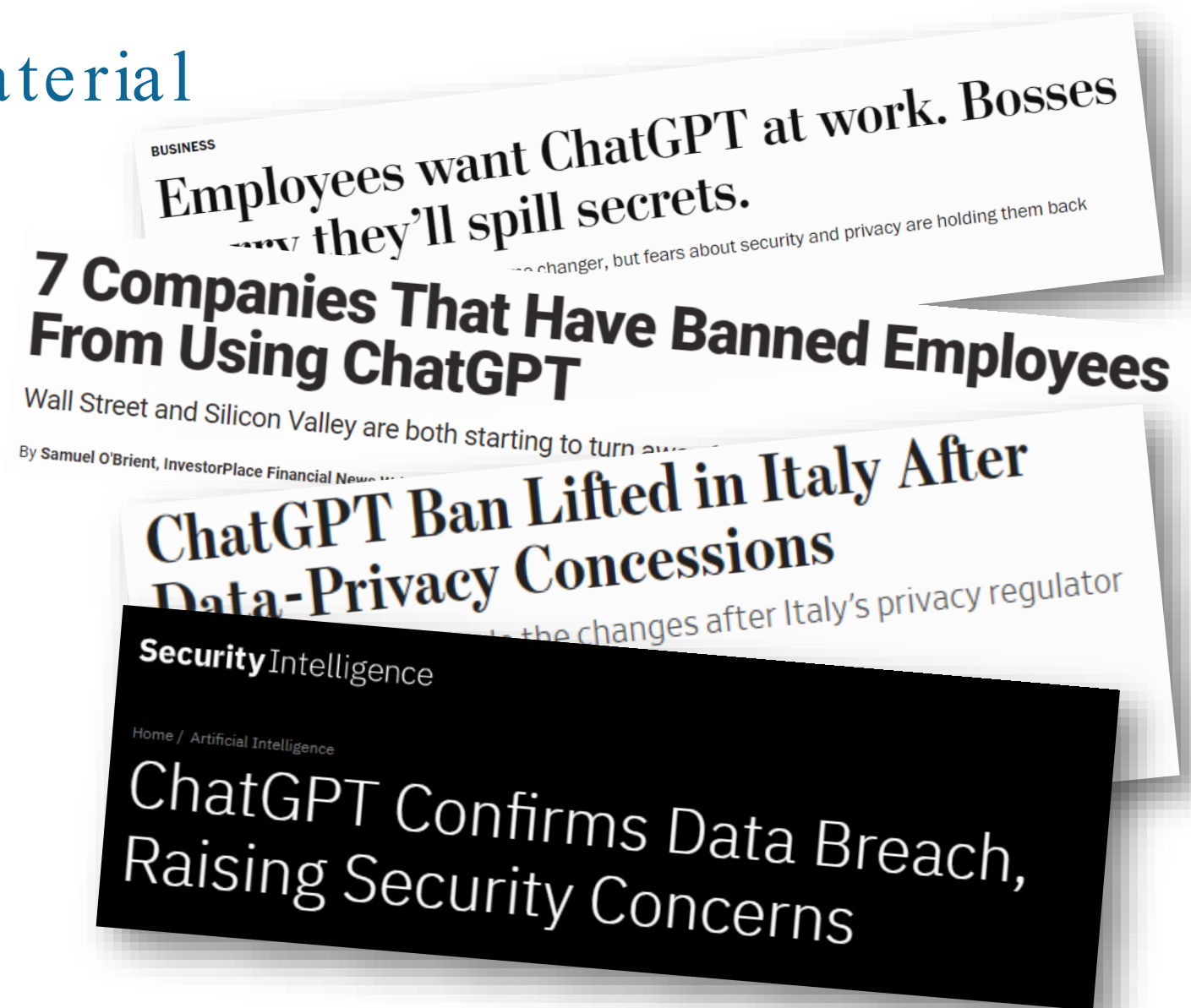
- Double-check for “Hallucinations”
- Use Multiple Tools
- Be Wary of Absolutes
- Avoid overreliance
- Learn how to prompt
- Recognize AI Bias
- Ask for Human Opinion
- Keep Updated on AI Developments



Disclosure of Sensitive Material

Best Practices

- Don't Input Sensitive Data
- Pre-Processing, Filtering
- Be Careful With Personal Conversations
- Awareness of Data Storage
- Learn About the Tool's Privacy Policy
- Establish Usage Policy



Copyright Issues

Best Practices

- Avoid Plagiarism
- Understand Fair Use
- Respect Creative Commons
- Clearance for Commercial Use
- Use Licensed Data
- Understand AI Generated Content Rights
- Create From Scratch
- Keep Records
- Seek Legal Advice

ChatGPT Creator Faces Multiple Lawsuits Over Copyright & Privacy Violations

ChatGPT maker OpenAI faces new class action lawsuit over data privacy

A new lawsuit against OpenAI could decide whether the company's use of training data scraped from the public internet may continue.



By Jon Gold

Senior Writer, Computerworld | JUN 29, 2023 1:38 PM PDT

Where Do We Go From Here?

Criminals will use it

GPS

It's a threat to jobs and will replace human workers

Personal computers

It's going to be the end of privacy and security

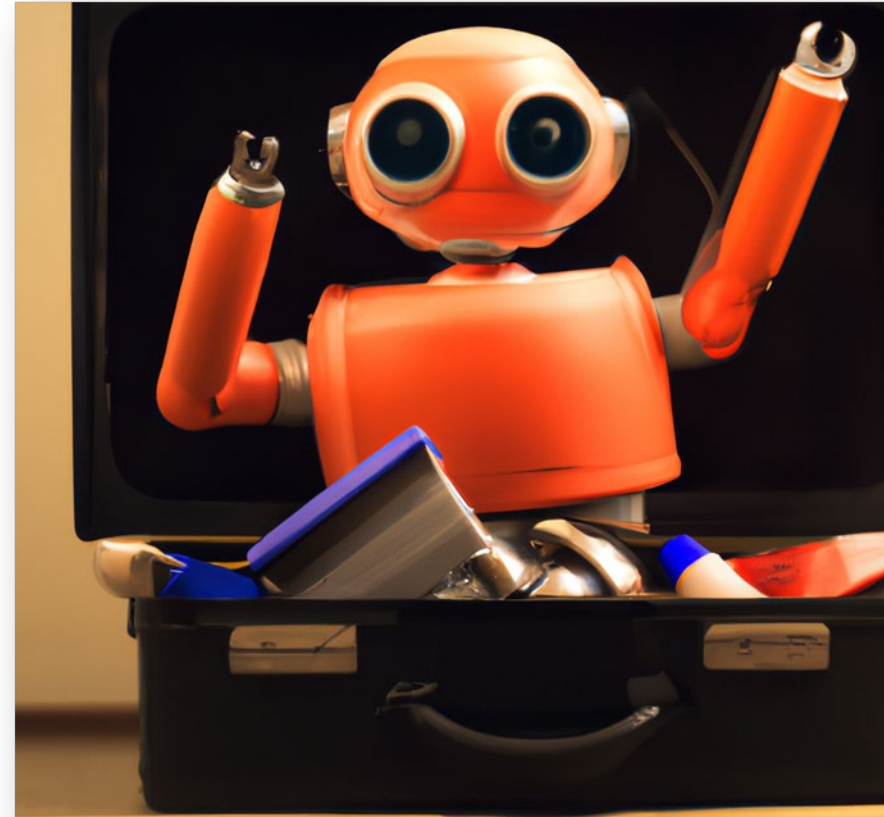
Cell phones

Questionable security and reliability

ATMs

Just Another Tool In The Toolbox

- Email
- Social Media
- Internet Browsers
- Wi-Fi
- Video Conferencing Software
- Generative AI



90-Day AI Strategy Plan

Forging an AI Future Now

First 30 Days:

- **AI Awareness** – Stakeholder identification and AI capability assessment.
- **AI Policy** – Details on what AI Tools the organization can or can't use (ex. ChatGPT). Educate employees on future governance and education.
- **AI Flash Assessment** – Leveraging the NIST AI Risk Management Framework (RMF).

30-60 Days:

- **Establish AI Committee** – Identify and gather key stakeholders to act as a governance, AI strategy, and implementation leadership team.
- **Evaluate AI Tools** – Determine best use and personas to utilize AI tools like Microsoft CoPilot in Microsoft 365, Dynamics, or ChatGPT Enterprise.

Forging an AI Future Now

60-90 Days:

- Tool Roll Out – Implementation and training for the AI tools selected.
- Pilot First AI Use Case – Develop and assess customized private use cases.
- Roadmap – Map Future AI use cases with AI Committee.

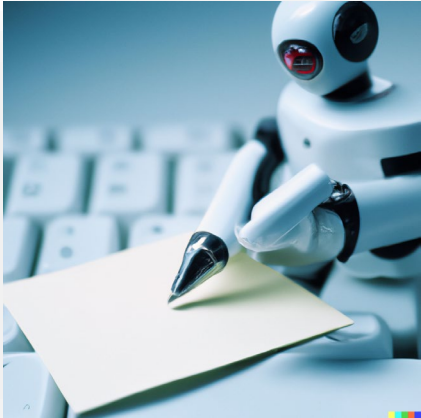
Beyond 90 Days:

- Scale and Revisit Strategy – Adjust strategies for successful AI initiatives.
- Long Term Vision – Conceptualize AI's future role in the organization.
- AI Full Gap Assessment – Consider an in-depth assessment against NIST AI RMF 1.0 covering all four functions and corresponding subcategories.

Recap

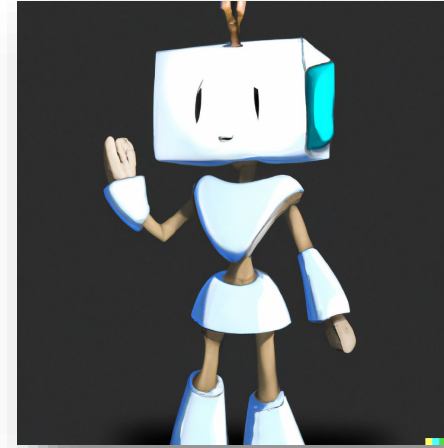
What is Generative AI:

- Software tool which can generate content based on input prompts.



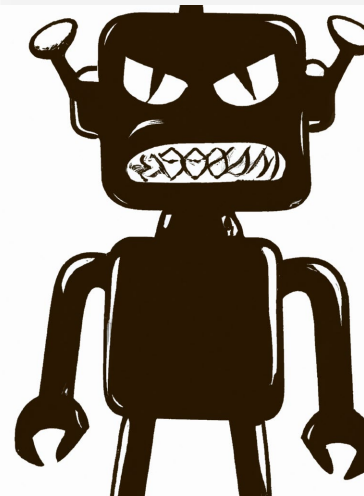
What Are The Risks:

- Unreliable results.
- Disclosure of sensitive information.
- Copyright Issues.



How Can We Use It:

- Assist in performing mundane tasks such as creating document templates.
- Expand our capabilities such as creating code.
- Expand our knowledge by answering questions.



A photograph of a modern glass-walled building with the letters 'LBMC' mounted on its upper facade. The building is set against a blue sky with wispy clouds. A bare tree is visible on the right side of the frame. A blue rectangular box with a white border is overlaid on the center of the image, containing contact information. Below the text box is a QR code. At the bottom of the image is a black horizontal bar with the website address in white.

Chris Collins

chris.collins@lbmc.com

(813) 759-3140



LBMC.COM