We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Artificial Intelligence: Walk – Governance & Security

March 13, 2024

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Today’s Presenters

Gregory Chambers, MCSE
Manager, Data Solutions
West Hartford, CT
860-570-6352
gregory.chambers@CLAconnect.com

Javier Young
Principal
Charlotte, NC
704-816-8470
javier.young@claconnect.com

Troy Hollings
Director, Data Analytics
Indianapolis, IN
317-567-6123
troy.hollings@claconnect.com

We Can Help You in 3 Ways …

Software *integration*

In-house products and solutions allow businesses to leverage leading value.

Data *modernization*

Every business relies on data insights to make accurate informed decisions.

Automation development

Adding automation to key processes allows businesses to scale efficiently.

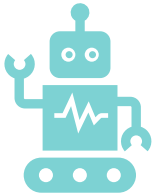
Protect your systems and data with a strong *cybersecurity* plan.

Crawl, Walk, Run Series: Artificial Intelligence

Crawl	Walk	Run
Understanding the AI Landscape	Governance & Security for AI Apps & Solutions	Advanced Solutions and Ethics

Today’s Agenda

Understand importance of data governance for AI



Explore Compliance & Cybersecurity Risks related to AI

Discuss policies and tools you can use to protect your organization’s data.

Review: Crawl Webinar

What Is GPT?

- GPT is a kind of Large Language Model: Able to generate novel, human-like text, write code, and create datasets
- Goal of GPT project was to create chat agent that can interact conversationally, generate coherent, relevant content, answer follow up questions.
- Trained on websites, books, and online material.
- Humans AI trainers helped GPT models provide more desirable outputs via reinforcement learning.
- OpenAI released ChatGPT November 2022
- Many updates & new generative AI apps & services, including Microsoft Copilot & custom solutions

Artificial Intelligence: Moving From Crawl To Walk

Data Governance and Risk Management Considerations

Characteristics of your Data Estate

- Data volumes
- System Complexity
- Digital TX Initiatives
- AI Apps & Solutions

Revenues | Costs | Risk | Agility

Digital Transformation

Governing Your Data Estate

Polling Question

What does data governance look like at your organization?

- Someone in Finance/Accounting spends a significant portion of their time focused on solving issues that arise.
- Finance, Operations, and IT work together on data governance and it's clear who owns our data and how to resolve issues.
- Oftentimes it feels like data anarchy, and I would like greater governance.
- I'm not sure.

AI Risk Management

AI Policy Considerations

- **Business strategy should inform the AI Policy.**
- **The AI policy should address:**
  - Legal and regulatory requirements
  - Acceptable AI usage, including generative AI usage
  - Quality, Security, Safety, Privacy
  - Risk Management
  - Roles and responsibilities
  - Impact to and from relevant third-parties

Polling Question

Do you use ChatGPT at work?

- All the time.
- A handful of times every month.
- I never have.
- We're not allowed to, and it's blocked.
- We're not supposed to, but it's not blocked.

What Could Go Wrong with Generative AI?

The dark web featured 225,000 sets of OpenAI credentials for sale in 2023 due to information stealers (scmagazine.com).

Access to sensitive data?

- PII

Intellectual property of companies

- Source code

Of data input into ChatGPT, 11% of that data posted by employees is considered confidential (cyberhaven.com).

Where’s the Data?

- For data used in AI models or applications, we should document:
  - What data is being use?
  - Where is data stored?
    - How is data stored?
  - How does data flow through the environment?
  - Who has access to the data?
    - How is access granted and removed?

Data Management and Administration

Consent and Collection

- Privacy laws often require consent from subjects by organizations before obtaining/using personal data.
- Transparency around usage of data for AI is generally required.

Minimization

- Organizations may only collect necessary data for intended AI purposes.
- This may limit training.

Data Retention

Privacy laws often require organizations to establish data retention policies and delete data that is no longer necessary.

This could affect AI systems that rely on historical data.

Artificial Intelligence and Cyber Risks

AI model manipulation

AI enhanced cybersecurity attacks

AI Deepfakes

Model Manipulation

- Indirect Prompt Injection Attack.
  - Attackers may be able to supersede a large language model's instructions to perform harmful/inaccurate responses.
- Corrupting data used for training AI models via data poisoning.

AI & Cybersecurity Attacks

- Threat actors are using Large Language Models to enhance their malicious activities.
- Activities include:
  - Information gathering
  - Interpreting technical documentation
  - Scripting
  - Social engineering
  - Impersonation
  - Evading security features

AI Deepfakes

- **“Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’” – CNN**
  - Fraudster invited employee to a video call where several deep faked “employees” were on, including the CFO.

AI Risks and Education

AI Risk Awareness Training should be provided to all employees at an organization at least annually, and at onboarding.

Enhanced training should be given to those with access to AI resources.

Governance, Security & Compliance in Practice

A brief survey of common AI tools

Governance & Security Platforms for AI

Tools should enable

- Centralized Data Management & Data Processing
- Data Cataloging
- Data Governance & Policy Compliance
- Security Administration
- Threat Monitoring

OpenAI's ChatGPT

ChatGPT

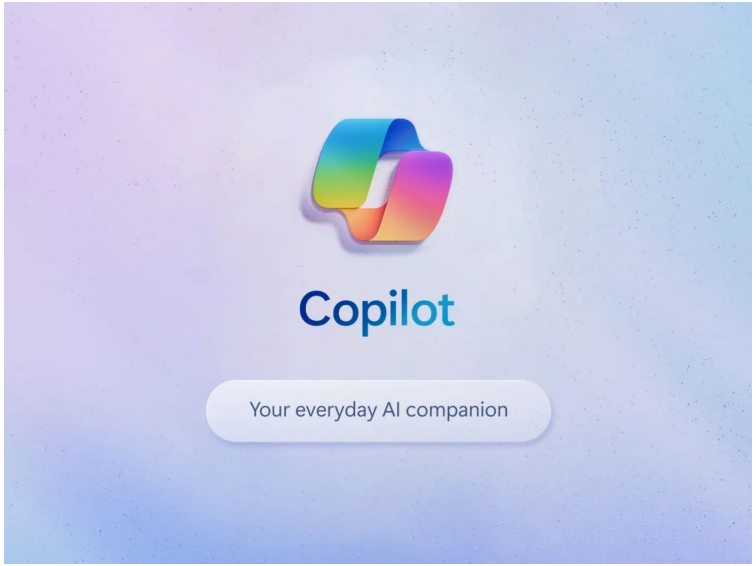
- ChatGPT Free & ChatGPT Plus collect any data entered by default for model training
- Turning off data collection is available
  - But also disables history of chats

ChatGPT Team & Enterprise

- Customer prompts or data are not used for training models
- Starts at $25/user/month (annual subscription)

Microsoft Copilots

- Data is temporarily stored by Microsoft.
- Data is not used to train models.
- Copilot Chat
  - ChatGPT-style addon to Microsoft 365 at $30/user/month



Other Tools

Microsoft Fabric

Data science

Data engineering

Data analytics

Microsoft Purview

Data governance, management & protection

Microsoft Security

Sentinel

Defender

Security Copilot – and more

Where to Go from Here?

3 Part Series – Crawl, Walk, Run – Artificial Intelligence	• Crawl – January 26, 2024 • Walk – Today • Run – May 15, 2024
Interested in discussing further?	• Click the “contact me for more information button”
Thanks again!	• gregory.chambers@CLAconnect.com • javier.young@claconnect.com • troy.hollings@claconnect.com

It takes balance.™

It’s our job to engage in conversations, listen to what you really want, and apply our talents and experience to make extraordinary impact on your organization and life.

Thank you!