*We'll get you there.*

CPAs | CONSULTANTS | WEALTH ADVISORS

# AI and Cybersecurity

Navigating the Benefits and Risks

Cybersecurity in the Age of Innovation

March 25, 2025

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.

# Learning Objectives

| | |
|---|---|
| Describe | Describe what Artificial Intelligence (AI) is and explore its many uses |
| Recognize | Recognize the potential benefits of AI and Automation |
| Discuss | Discuss AI risks as well as risk management for AI use |

# What is Artificial Intelligence?

# My Background

Javier Young, CISSP

Principal – Cybersecurity

Over 15 years of experience in the cybersecurity field providing IT security, risk, and consulting services to clients in healthcare, higher education, and financial related institutions.

# Optimization

## *Traffic Pattern Analysis*

- Ad-hoc traffic analysis via sensors
- Midtown Atlanta
- Predictive analytics on traffic trends
- Optimization of routes

## *Biometric Authentication*

- Using Iris codes for authentication
- Many variables to consider with Iris code authentication

# Evolutionary Computing

## *Darwinism of the Data*

- Survival of the fittest!

## *Genetic Algorithms*

- Initialization
- Evaluation
- Selection
- Crossover
- Mutation
- Stop criteria

# AI for Benefit

# Productivity Tool

- Generative AI
- Automate decisioning in tasks
- IoT devices
- Smart homes
- Data entry
- Expense categorizing
- GitHub CoPilot
- Creating this presentation

# Tax Preparation

Today multiple software packages can do individual returns

What if, as an organization, you were able to input all corporate tax laws into software and click ‘Do Taxes’?

For corporations, would this not be the ultimate accountant?

- CPA 2.0?

# Process Automation

- Leveraging Robotic Process Automation Technologies (RPA)
  - Data transfers
  - Reaching into multiple systems to update records and handle customer communications
  - “Reading” documents to extract provisions using natural language processing
- The Harvard Business Review analyzed 71 RPA projects [… and] replacing administrative employees was neither the primary objective nor a common outcome

# Predictive Analytics

Market basket analysis

Staff need forecasting

Reducing hospital readmission rates

Personalized financial services needs/products

# AI Governance and Risks

# AI Policy Considerations

Business strategy should inform the AI policy

The AI policy should address:

- Legal and regulatory requirements
- Acceptable AI usage
- Quality
- Security
- Safety
- Privacy
- Risk Management
- Roles and responsibilities
- Impact to and from relevant third-parties
- Generative AI usage

# Gemini, ChatGPT, Watsonx Generative Application

## Generative output based on user input

- Understanding of intent defined by Natural Language Processing and Large Language Models
- Depending on use case text, image, audio, video, and code can be generated, based on a user's request

## At a high level, Generative AI supports:

- IT DevOps
- Entertainment
- Education
- Finance
- Healthcare
- Human Resources

## Support and optimization from an internal-facing and client-facing perspective

# 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).

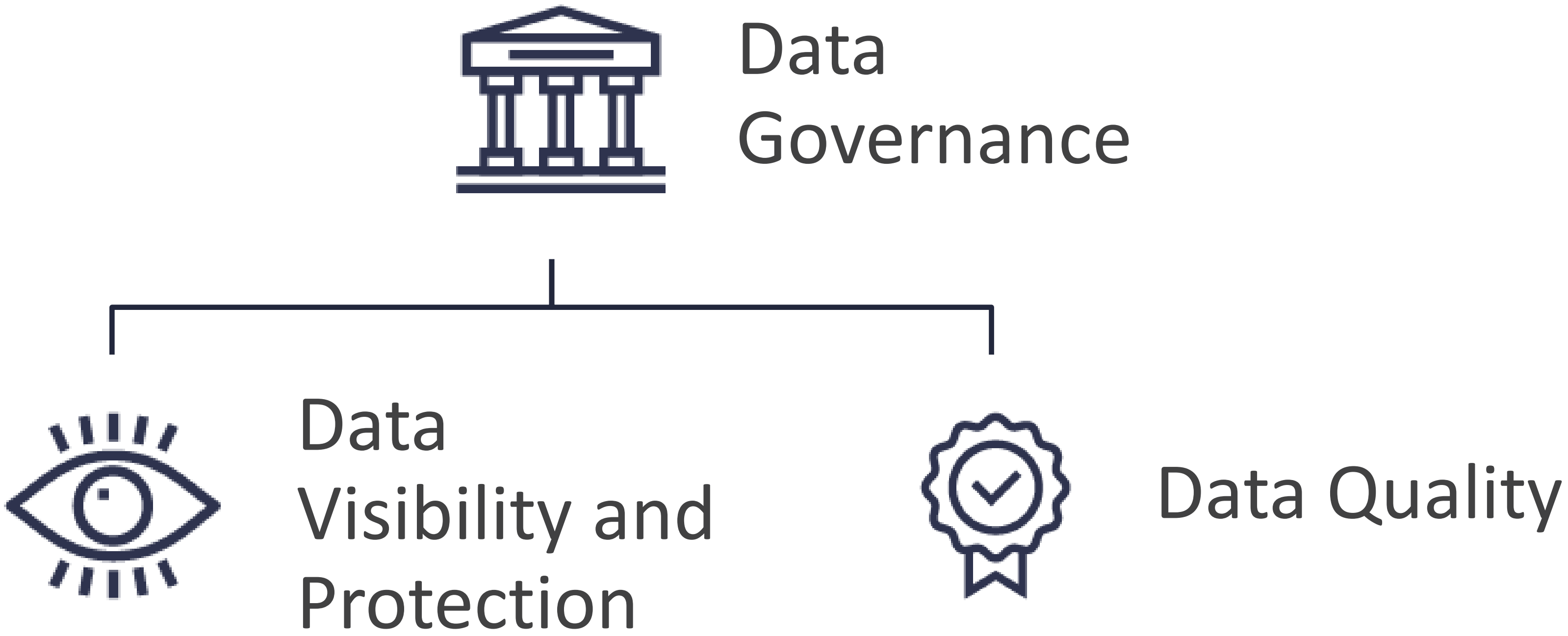
- Access to sensitive data?
  - PII
- Intellectual property of companies
  - Source code

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

# AI Regulations

- There has been consensus around AI needing regulation to protect the data privacy.
  - ISO IEC 42001:2023
  - NIST AI RMF 100-1
  - EU AI Act (In progress)
  - H.R.2701 – 118TH Congress – Online Privacy
  - GDPR
  - CCPA

# Governing Your Data Estate



Data Governance

Data Visibility and Protection

Data Quality

# How are States Currently Regulating AI?

- Over the past five years, 17 states have enacted 29 bills that focus on AI regulation align with these principles
  - Of these bills, 12 have focused on ensuring data privacy and accountability
  - This legislation hails from California, Colorado, Connecticut, Delaware, Illinois, Indiana, Iowa, Louisiana, Maryland, Montana, New York, Oregon, Tennessee, Texas, Vermont, Virginia and Washington

# 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 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.

# Managing Risks

# User and Entity Behavior Analytics

Use analytics to detect anomalous behaviors

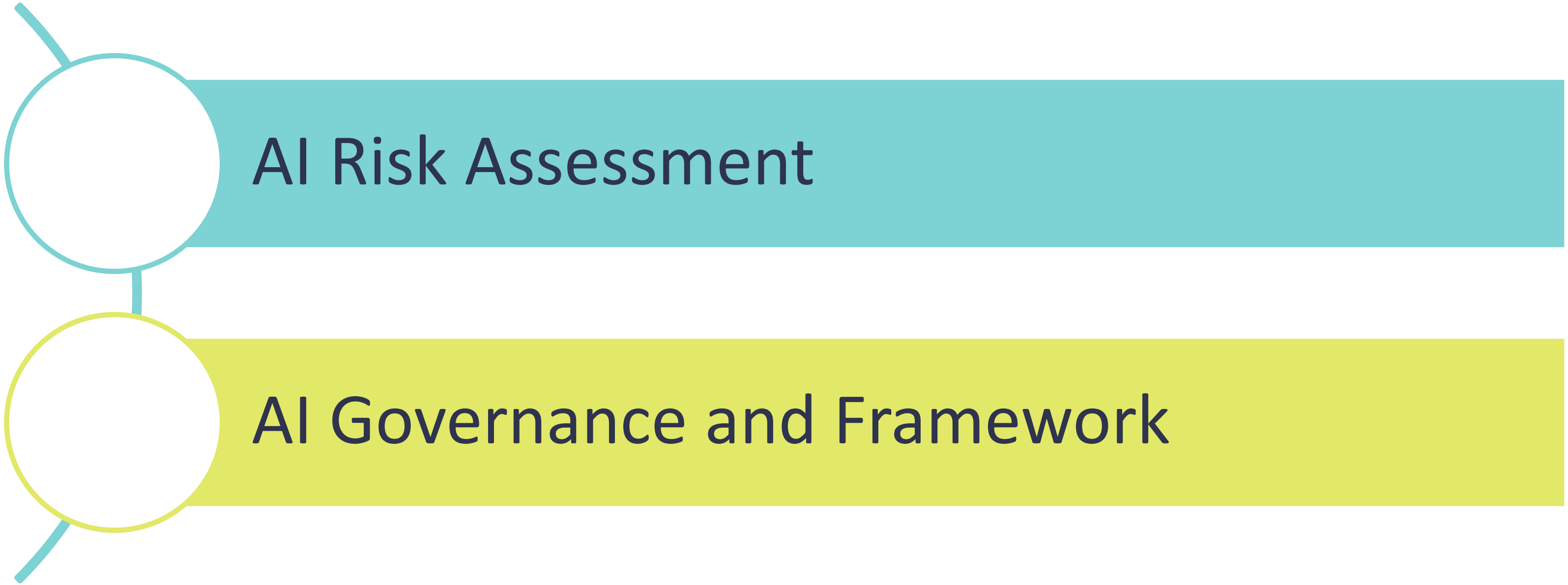
Baseline normal to detect abnormal

Profile user behaviors and alert on suspicious activity

Auto analyze network traffic trends

Profile workstation and endpoint activity

# Be Proactive!



AI Risk Assessment

AI Governance and Framework

# *Thank You!*

Javier Young
Principal – Cybersecurity
704-816-8470
javier.young@CLAconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS