



# Leveraging AI in the financial environment

Panel Discussion

# Brandi Manna, CPA

*Senior Manager*

[bmanna@troutcpa.com](mailto:bmanna@troutcpa.com)

717-358-9018

## Practice Areas

- › Outsourced Accounting
- › Outsourced Controller

## Education

- › BS in Accounting – Pennsylvania State University, Capital College
- › Certified Public Accountant - 2012

# Nikelle Druck

*Director of Client Accounting Services*

[ndruck@troutcpa.com](mailto:ndruck@troutcpa.com)

717-283-5974

## **Practice Areas**

- › Outsourced Accounting
- › Data Analytics
- › IT & Professional Consulting

## **Community Involvement**

- › Manheim Township Dugout Club - Board Treasurer
- › Meals on Wheels - Board Member

# Tim Barley

*Integration Developer*

[tbarley@troutcpa.com](mailto:tbarley@troutcpa.com)

717-358-9010

## **Practice Areas**

- › Process Automation
- › Data Analysis
- › Application Development
- › Service Integrations

# Chris Bomberger

*Director of Information Technology - AVAIL*

[cbomberger@availnow.com](mailto:cbomberger@availnow.com)

<https://www.linkedin.com/company/availnow/>

## Professional Areas of Focus

*VCISO, Security, and Cloud Infrastructures Solutions*



# QUESTION #1

What are the advantages of leveraging AI in the finance and accounting industry?

# GEMINI RESPONSE

- **Improved accuracy and efficiency:** AI can automate many routine tasks such as data entry, reconciliation, and fraud detection. This frees up human accountants to focus on more complex work that requires judgment and expertise.
- **Enhanced fraud detection:** AI can analyze vast amounts of financial data to identify patterns and anomalies that might indicate fraudulent activity. This can help organizations prevent fraud before it occurs or minimize losses.
- **Deeper financial insights:** AI can analyze financial data to identify trends, risks, and opportunities that might be missed by human analysts. This can help organizations make better decisions about everything from resource allocation to investments.
- **Improved regulatory compliance:** AI can help automate compliance processes and ensure that financial institutions are meeting all regulatory requirements. This can save organizations time and money and help them avoid penalties.
- **Stronger customer service:** AI-powered chatbots and virtual assistants can provide 24/7 customer service and answer basic financial questions. This can improve customer satisfaction and reduce the workload on human customer service representatives.

## QUESTION #2

What are some day-to-day challenges when it comes to leveraging AI?



# GEMINI RESPONSE

- **Data Bias:** AI algorithms are only as good as the data they're trained on. If the data is biased, the AI system will also be biased, leading to unfair or inaccurate results. This can be a real concern in finance, where decisions can have a big impact on people's lives.
- **Data Quality and Management:** AI systems require a lot of high-quality data to function properly. Cleaning, validating, and integrating data can be a complex and ongoing process. Without this, AI models may not be reliable.
- **Explainability and Transparency:** Sometimes, it can be difficult to understand how AI systems reach certain conclusions. This lack of transparency can make it difficult to trust the AI's recommendations, especially for critical financial decisions.
- **Change Management:** Implementing AI can lead to significant changes in how work is done. This can be disruptive for employees and requires effective change management strategies to ensure user adoption.
- **Security Risks:** AI systems can be vulnerable to hacking and other security threats. It's important to have robust security measures in place to protect sensitive financial data.

## QUESTION #3

What are the security and risk factors that people in technology are trying to combat for client service industries such as outsourced accounting and IT providers?

## Data Security Risks

- **Unauthorized access to client data:** Hackers and malicious insiders are constantly looking for ways to steal sensitive information, such as financial data, personal identifiers, and intellectual property.
- **Accidental data loss:** Human error and system failures can also lead to the loss of client data. This can be just as damaging as a cyberattack, as it can still result in financial losses and reputational damage.
- **Data breaches:** Data breaches are caused by vulnerabilities in IT infrastructure, such as weak passwords or outdated software. They can also be caused by social engineering attacks, where attackers trick employees into giving them access to sensitive data.

## Access Control Risks

- **Inadequate access controls:** If access controls are not properly configured, unauthorized users may be able to access sensitive data. This can happen if employees are given more access than they need to do their jobs, or if there are no controls in place to prevent unauthorized access from outside the company.
- **Weak password policies:** Weak password policies make it easier for attackers to steal credentials. Hackers can use brute force attacks or password spraying techniques to guess passwords.
- **Insufficient monitoring of user activity:** Companies need to monitor user activity to detect suspicious behavior. This can help to identify potential security breaches and prevent them from happening.

## Compliance Risks

- **Failure to comply with industry regulations and data privacy laws:** There are a number of industry regulations and data privacy laws that client service industries need to comply with. These laws can vary depending on the industry and the jurisdiction. Failure to comply with these laws can result in hefty fines and reputational damage.
- **Data breaches that result in hefty fines and reputational damage:** Data breaches can also lead to hefty fines and reputational damage. Companies that suffer data breaches may lose the trust of their customers and partners.

## Third-Party Risks

- **Security vulnerabilities in the systems of third-party vendors:** Client service industries often rely on third-party vendors for a variety of services, such as data storage and cloud computing. Security vulnerabilities in the systems of these vendors can put client data at risk.
- **Data breaches at third-party providers that expose client data:** Data breaches at third-party providers can also expose client data. Client service industries need to carefully assess the security practices of their third-party vendors before doing business with them.
- **Lack of control over how third-party vendors handle client data:** Client service industries often have limited control over how third-party vendors handle their client data. This can be a risk, as there is no guarantee that third-party vendors will have the same security standards as the client service industry itself.

## QUESTION #4

Do you have any specific policies that have been adopted or are in progress to mitigate against the challenges with AI data security breaches?

# GEMINI RESPONSE

## Focus on data security throughout the AI lifecycle:

- **Data minimization:** This principle encourages collecting only the data essential for the AI's function, reducing the attack surface and potential damage from a breach.
- **Data anonymization and pseudonymization:** Techniques like anonymization (removing identifiers) and pseudonymization (replacing identifiers with aliases) can protect sensitive data while allowing AI development.
- **Data encryption:** Encrypting data at rest and in transit adds an extra layer of security, making it harder for attackers to exploit even if they gain access.



# GEMINI RESPONSE

## Securing AI models themselves:

- **Adversarial training:** This involves exposing the AI model to deliberately corrupted or manipulated data during training, helping it identify and resist such attacks in the real world.
- **Model monitoring and auditing:** Regularly monitoring AI models for bias, drift (unexpected changes in behavior), and security vulnerabilities is crucial for maintaining trust and preventing issues.

# GEMINI RESPONSE

## Improving governance and accountability:

- **Standardized AI security frameworks:** Industry-specific or government-backed frameworks can provide clear guidelines on secure AI development and deployment.
- **AI ethics guidelines:** These guidelines can address responsible data collection, use, and potential biases to mitigate risks and build trust with users.

# GEMINI RESPONSE

## Utilizing AI for AI security:

- **AI-powered threat detection:** AI can be used to analyze vast amounts of data to identify suspicious activity and potential breaches in real-time.
- **Automated security patching:** AI can streamline the process of patching vulnerabilities in AI systems and connected infrastructure, reducing the window of opportunity for attackers.

# GEMINI RESPONSE

It's important to remember that these policies are still evolving. The field of AI security is constantly growing, and new challenges and solutions will emerge as AI technology continues to develop.