falling victim to common pitfalls related to unwanted data exposure.

Jan. 09, 2024

By Shane Westra.

In recent years, the integration of Artificial Intelligence (AI) and Machine Learning into accounting firms has been on the rise, bringing both opportunities and challenges. As these technologies become more embedded in daily operations, it is crucial to keep a balanced perspective, particularly regarding the security of sensitive data. Protecting client information is of utmost importance in this evolving landscape.

Here are some key points to help you leverage the benefits of AI in your firm without

measures. Begin by setting up transparent and well-defined protocols for sharing data. Enforce stringent controls on who can access data, and ensure that data is encrypted when being transferred. Additionally, make sure that any contracts with third-party entities explicitly address data confidentiality and include obligations for conducting security audits and providing regular reports.

Proactively secure data to maintain confidentiality. To maintain data confidentiality, you need to protect information from unauthorized access while you are sending the data as well as when it is stored on local hardware.

While integrating AI tools into your firm's workflows can be smooth, it is vital to stay aware of the risks to prevent inadvertent exposure of sensitive information. It is important to comprehend the potential risks associated with the particular AI applications used in your firm, especially how they handle, store, or possibly distribute sensitive internal and client data.You will likely need to contact the developer of the AI applications you are using to receive detailed answers.

Understand how the AI tools you use retain data. AI tools may store data to train their natural language model or to share your input data with third parties. As a result, any data input into the solution may expose your confidential information to unauthorized parties. Always make sure to check your AI tool's retention and sharing policies to make sure your data is not stored for future use and that you are able to comply with IRS and other security regulations and privacy standards.

Even when an AI tool meets compliance standards, it is essential for your firm to have a strong security system that encrypts data to prevent unauthorized access or interception. Before implementing any technology, thoroughly question the solution developer to ensure that its features don't introduce excessive risk to your firm. Maintaining the trust and confidentiality of your clients and stakeholders depends on this due diligence.

Learn how to respond to AI-driven data compromises. If your data is compromised

In the event of a data breach affecting your client's data, regardless of whether it is related to AI, you should inform your clients promptly. Following this, adopting and enforcing best practices for managing and storing sensitive information is essential. Such actions are key to enhancing and potentially rebuilding trust in your client relationships.

As accounting and finance continues to evolve and embrace AI-driven solutions, it is essential to expand your skill set in these areas to stay current and competitive.

Develop an AI usage policy incorporating governance, confidentiality and data integrity. If your firm has not alreadyestablished comprehensive AI usage policies that address concerns related to AI and data governance, confidentiality, availability and integrity, now is the time to put this framework in place.

An effective AI usage policy should start with a clear vision of the responsibilities of each member of your team (both internal and external parties) for overseeing AI adoption and usage as well as the processes for monitoring and assessing the risks associated with it. This should include a dedicated team or individual responsible for overseeing all AI initiatives and ensuring compliance and data confidentiality.

A comprehensive data confidentiality policy should also outline strict access controls and data encryption requirements for the usage of AI tools. One of the primary outcomes of adherence to this policy is that only authorized users can interact with the systems in your firms that touch sensitive data and also those incorporating AI tools. Working closely with AI-powered solution vendors can help ensure that your firm's data protection standards are upheld and that they can provide the necessary data security controls.

Accounting for AI in the future. AI is here to stay in the accounting profession. Firm leaders must remain adaptable and proactive in addressing new data security

challenges stemming from the sea change that has occurred with the introduction of

Shane Westra is a product manager at Canopy and has 20+ years of experience leading Product and R&D teams for high-profile SaaS companies such as LexisNexis, Pearson, Workfront (now part of Adobe), Shutterstock (Bynder), and nCino (SimpleNexus). Whether in Salt Lake City or Silicon Valley, Shane has consistently helped both growth-stage and mature companies define their strategic vision, build innovative products and platforms, and level-up industries with modern tools.

Artificial Intelligence • Firm Management • Technology