Hey! What’s New? 2025-40

Shadow AI – Rising from the Penumbra

Mark Horseman writes in the latest issue of *The Data Administration Newsletter* that “in the last couple of years, AI has taken over our organizations. While the benefits of using AI to augment your organization’s ability to achieve its business goals are abundant, the risks associated with unmanaged AI use are many. To add further strain on the use of AI within organizations, sometimes it sneaks its way in. Enter shadow AI.”

Horseman notes that “one of the impacts of shadow AI observed in organizations is when well-meaning employees implement their own AI solution without necessarily divulging that use to the organization. Depending on the use case, this can be using something like ChatGPT to help write a proposal or analyze data.”

While a Large Language Model (LLM) can do a fantastic job with tasks like these, Horseman finds that the risks to the organization are many. “Is there confidential information in the prompt or response? Providing clear procedures and guidelines for folks within our organization is key to preventing issues to hidden AI use.”

While some organizations choose to simply turn off all access entirely, he believes that this will not prevent the use of AI, “as users happen to be a crafty lot.” So, “the shadows can still creep up on us. People bring phones to work these days, along with many other ways to get to resources outside the corporate firewall. Instead of prohibiting the activity and forcing it underground, having clear policies, procedures and guidelines in place to help and enable will do a lot more to de-risk AI in an organization.”

Another area of shadow AI is when it is an undocumented (or under-documented) feature in Commercial off-the-shelf (COTS) software solutions. Horseman says that “in various AI governance frameworks, including where an AI review in the requisition process is present, you may want to consider something like this for your organization’s policy. If left unconsidered, some software solutions could be using your data to train a model without your knowledge. Depending on the nature of your business, this could vary in risk from a slight annoyance to massive fines. Also, having a review in place for commercial software can also discover cases where a tool may advertise something is AI powered, but it is merely a clever algorithm that does no actual learning or training at all, which would highlight a vendor that claims their solution does more than it really does when implemented.”

Horseman suggests that “our most potent tool to manage AI is the trusty policy, which is backed by procedures and guidelines. Even if your organization is not typically managed by policy, writing out what a policy framework would look like is a helpful exercise. Key things we need to define and document as it relates to governing AI in our organizations are as follows:

- **AI Owner:** Ultimately, who in your organization is responsible for the operation and results of the AI implementation?
- **AI Model:** What is the model we’re running, the specific LLM or the algorithm at play? Also, how was it trained? Is there bias in the model?

- **Risk:** What is the risk to our organization when it comes to the results of the AI model? Will we recommend a product to a customer who isn't interesting? Is there potential reputational risk if bias isn't considered? Could we end up in the news or fined because of our use of AI?
- **Security**: Do the results of AI stay local, is our interaction with AI and its results being shared and used to train that model for other sources?
- **Use**: Is this AI tool embedded in an existing solution? What business processes is it being used in?

There are many other factors we could consider, Horseman notes, "and you'd want to be specific about what you need to document. When writing a policy, you want to focus on the high-level beliefs of your organization. When you support that policy with procedures, you want to include the rules related to how that policy is put in place, that's where the above documentation rules become a critical factor. What exactly do we document and how do we make that available in our business, but also, how do we ensure that all our AI usage follows our documentation procedures? Putting in place the rigour to do these things will save your organization."

For more have a look at Shadow AI – Rising from the Penumbra – TDAN.com.