Agentic AI and the Coming Apocalypse

April 6, 2026 - We've all heard the stories about how AI is going to kill us all. It's going to be smarter than we are. It's going to get things done faster and more accurately than we do. It's going to take over the world and say, "Hey, we don't need these HUMANS anymore!" But that's at least a few years away. Before that happens though, it is likely to cause some real business and privacy disasters because of what is being called agentic AI. And we're likely to start seeing some of those things within the next 12 months.

In the event you haven't heard of agentic AI, it is simply AI that gets work done on your behalf. Anthropic's Claude probably has the best-known versions of it. Claude has an agent called Cowork. You can tell the agent what you want done and it becomes Cowork's job to figure out how to get it done. Given my experience with AI, I'm pretty sure that is going to lead to some erroneous data being circulated in corporate America, but that's another story.

Companies are building agents at a rapid pace. And some of these agents can actually take over a user's computer, giving the agent access to files and software, launching programs, sending commands, etc... Pretty much anything you can do on your computer, there's an agent that can do it for you and it may be faster and better at doing it than you are. But therein lies the issue. Who's controlling that agent? And what is that agent being told to do?

You don't have to be a rocket scientist to figure out that this can create real issues. Agents are being rolled out and installed by employees to do their work. And companies often have computer security policies that aren't quite up to snuff. What could possibly go wrong?

Well, let's think. Let's say you have an employee who is thinking about moving to a new company for a promotion or just better pay. He instructs and agent to copy your customer database and send it to an email address. Or let's say you have an employee who just wants to know what everyone else in the company is being paid. They can send an agent to gather that information and maybe make it public. Or how about a worst-case scenario. You have a disgruntled employee that tells an agent to wipe out your customer database. That could put you out of business.

The companies that making these AI agents all appear to be in a rush to get their products to market. But the safety controls for agentic AI really aren't well understood. In fact, you have a lot of people in corporate America that are looking just at the efficiencies that AI can bring to their businesses without considering the downsides. And the issue is complicated by the fact that many of the people making decisions about AI use don't really understand how AI works.

Complicating matters even more, you have a number of well known and lesser-known companies that are making AI agents and the competition is stiff. They all seem like they are more interested in market share than they are in safety protocols. That's just an opinion but given what I've seen in the market, it's an informed opinion.

The pressure for businesses to use AI is very real. But businesses need to understand what they are doing and put some safety guard rails in place before they get carried away. The is true for both large and small companies. Not doing so will almost certainly lead to some business disasters, embarrassment, privacy breaches, etc... in the very near future.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS