AIM

AIM CYBER

High-touch services to help you navigate modern cyber threats.

AI AND ML HAVE BENEFITS BUT ADD TO RISKS

We are bombarded with ads and articles about new technologies and how they will solve our problems. And it has been going on for decades if not longer.

The latest ones are Artificial Intelligence, AI, and Machine Learning, ML. While similar and related there are differences.

AI is defined as any system that perceives its environment and takes actions that maximize its chance of achieving its goals. AI is used for tasks that require human intelligence such as thinking, reasoning, learning from experience, and most importantly, making its own decisions.

ML is defined as is the study of computer algorithms that can improve automatically through experience and by using data. ML is a subset of Artificial Intelligence.

AI and ML offer benefits but also add to cyber risks. What are you turning over to AI and ML? Business decisions, selections, potential candidates for employment, approving or denying insurance claims, medical diagnoses and so many other things.

The reliance on these systems is increasing both in terms of the number of processes relying on AI and ML, and increased autonomy of the system without human intervention.

Productivity improvement? Probably. Cyber risk with potential damages? Definitely.

Consider the business impact of the decisions or choices being made by these systems. Now think of the damage that can be done, financial, reputational, legal, etc. if these systems are hacked.

Hacking doesn't have to damage the system. If fact the outcomes will be worse if the systems are left operating, but the algorithms and other decision-making mechanisms are changed.

Let's use an insurance company as an example. If the risk assessment for underwriting is changed, cybercriminals can issue policies to friends for much lower premiums than needed or to people who wouldn't qualify. Now, let the claim system algorithms or decision making be changed to automatically approve any claim by these policy holders. How many millions of dollars will be paid out before red flags are raised?

This is just one example. And the hacking doesn't have to be on your system, it can be a supply chain hack similar to SolarWinds where the AI or ML system you use gets hacked and distributed in updates from the vendor. Or to the AI or ML system if in the cloud.

We are certainly not suggesting you avoid the use of AI and ML systems; they offer too much potential benefit. But we are suggesting you look at the additional risks these systems add. Then redefine the alerts and the oversight to catch problems before they wreak havoc.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.