AI GATHERING YOUR DATA

BY JAY BORDEN

As we have written before, Generative AI systems and Chatbots are proliferating at a staggering rate. As is their use.

Companies are implementing them for multiple purposes, for employees to offload mundane or repetitive tasks, and more. That can be beneficial. However, remember that for the AI system to generate anything, it has to have input. Need a presentation, input the material you want in the presentation. Want a report, input the data or other information needed. Want an analysis of large amounts of data, input the large amounts of data. You get the picture.

That part makes perfect sense. How can the AI system write the report or presentation or do the analysis without the initial information or data?

The problem is that once the Generative AI system is made available, no one monitors what employees do with it, how they use it, or what information is input.

Few people know that the AI systems keep what is entered. It is supposedly for them to "learn." However it may be explained, the information is now in the AI system. Much of it is proprietary and may even be protected by laws. It may be company confidential information about strategy. It may be medical information about patients. It may be any form of Personally Identifiable Information. None of which was ever intended to be released outside the company.

But it has been. Inadvertently, it is true. But that won't help if your competitors see it and know how to defeat you. Of if regulators see the protected data and impose fines. Saying you didn't know it was being saved by the AI system won't cut it.

If company strategic direction and facts are released it can mean the end of the company. Even if it is not the end of the company, it will certainly impact earnings and customer trust.

onebrightlycyber.com
(888) 773-1920

INFOSTEALERS – PREDECESSOR TO RANSOMWARE ATTACKS

CONTINUED

If it is customer information or a presentation to a customer or new prospect, do you think they will stay or choose to do business with you?

If it is PII or protected health information, you may well be fined. But will your customers or patients leave?

Whatever way you view this, it will not be good. The results and impact can range from a minor inconvenience to a major disaster.

But like Pandora's box in mythology, once it is opened, it is impossible to get the evils back inside. Take a close look at who has access to the AI system and how they are using it. Has there been any training or other guidelines or regulations pertaining to the use of the AI system? Has everyone who has access to the AI systems successfully completed the training? Do they understand the implications of non-compliance? Is any monitoring of their use in place? Are penalties in place for failing to follow the regulations?

Be sure you answer those questions honestly. The future of your company may well depend upon the answers and what you choose to do.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.