JAVELIN

Reducing the Noise of AI in Cybersecurity

01 June 2020 By: Krista Tedder

To augment the lack of staffing and reduce risks, financial services cybersecurity teams are bombarded by artificial intelligence-based solutions (AI) that they are told will solve all of their problems. But the reality is that AI may cause more problems for chief information security officers (CISOs) and impede their ability to be agile in a rapid and dynamic environment.

AI has tremendous potential when it comes to cybersecurity, but it is not a silver bullet or a replacement for proper cybersecurity risk management. CISOs have a dual role when it comes to AI. They need to leverage the technology as part of core cybersecurity activities, as well as secure AI deployments throughout their organizations. Doing so will improve the security maturity of the organizations they support. This report covers cybersecurity use cases where AI can help, attacks on machine learning algorithms, pitfalls to avoid, and a list of questions to help cybersecurity leaders evaluate AI solutions.

Key questions discussed in this report:

- How does AI help create more mature cybersecurity organizations?
- What are the threats and pitfalls cybersecurity teams should be aware of when it comes to deploying AI?
- How should cybersecurity AI tools be evaluated? What questions should be asked to providers?

Enterprise data in this report was collected from an online survey, conducted in May 2020, of 506 cybersecurity leaders for businesses headquartered in the United States.

javelinstrategy.com inquiry@javelinstrategy.com 925.225.9100