lavery
Lawyers

Improving Cybersecurity with Machine Learning and Artificial Intelligence

June 5, 2020

Author

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

New challenges

The appearance of COVID-19 disrupted the operations of many companies. Some had to initiate work from home. Others were forced to quickly set up online services. This accelerated transition has made cybersecurity vitally important, particularly considering the personal information and trade secrets that might be accidentally disclosed.

Cybersecurity risks can stem not only from hackers, but also from software configuration errors and negligent users. One of the best strategies for managing cybersecurity risks is to try to find weak spots in the system before an attack occurs, by conducting a penetration test, for example. This type of testing has really evolved over the past few years, going from targeted trial and error to larger and more systematic approaches.

What machine learning can bring to companies

Machine learning, and artificial intelligence in general, is able to simulate human behaviour and can therefore function as a hypothetical negligent user or hacker for testing purposes. As a result, penetration tests involving artificial intelligence can be a good deal more effective.

One example of relatively simple machine learning is Arachni: open-source software that assesses the security of web applications. It is one of the tools in the Kali Linux distribution, which is well-known for its penetration testing. Arachni uses a variety of advanced techniques, but it can also be trained to be more effective at discovering attack vectors-vulnerabilities where the applications are the most exposed.[1] Many other cybersecurity software programs now have similar learning

capabilities.

Artificial intelligence can go even further. Possible uses for artificial intelligence in the cybersecurity field include[2]:

A faster reaction time during malware attacks
More effective detection of phishing attempts
A contextualized understanding of abnormal user behaviour

IBM has recently created a document explaining how its QRadar suite, which incorporates artificial intelligence, can reduce managers' cybersecurity burden.[3]

What it means:

Human beings remain central to cybersecurity issues. Managers must not only understand those issues, including the ones created by artificial intelligence, but they must also give users clear directives and ensure compliance.

When considering which cybersecurity measures to impose on users, it is important for IT managers to be aware of the legal concerns involved:

Avoid overly intrusive or constant employee surveillance. It may be wise to consult a lawyer with experience in labour law to ensure that the cybersecurity measures are compatible with applicable laws.
It is important to understand the legal ramifications of a data or security breach. Some personal information (such as medical data) is more sensitive, and the consequences of a security breach involving this type of information are more severe. It may be useful for those responsible for IT security to talk to a lawyer having experience in personal information laws.
Finally, a company's trade secrets sometimes require greater protective measures than other company information. It may be wise to include IT security measures in the company's intellectual property strategy.

---

1. https://resources.infosecinstitute.com/web-application-testing-with-arachni/#gref
2. https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/; https://towardsdatascience.com/cyber-security-ai-defined-explained-and-explored-79fd25c10bfa
3. *Beyond the Hype, AI in your SOC*, published by IBM; see also: https://www.ibm.com/ca-en/marketplace/cognitive-security-analytics/resources