THE RISKS AND BENEFITS OF USING AI TO DETECT CRIME

Companies are using it for everything from routine theft to insider trading

Lisa Quest, Anthony Charrie, and Subas Roy

COMPANIES ARE USING artificial intelligence (AI) to prevent and detect everything from routine employee theft to insider trading. Many banks and large corporations employ AI to detect and prevent fraud and money laundering. Social media companies use machine learning to block illicit content like child pornography. Businesses are constantly experimenting with new ways to use artificial intelligence for better risk management and faster, more responsive fraud detection, and even to predict and prevent crimes.

While today's basic technology is not necessarily revolutionary, the algorithms it uses and the results they can produce are. For decades, banks have been using transaction monitoring systems based on predefined binary rules that require the output to be manually checked. The success rate is generally low: On average, only 2 percent of the transactions flagged ultimately reflect a true crime or malicious intent. By contrast, today's machine-learning solutions use predictive rules that automatically recognize anomalies in data sets. These advanced algorithms can significantly reduce the number of false alerts by filtering out cases that were flagged incorrectly, while uncovering others missed using conventional rules.

Given the wealth of data available, and the rising expectations of customers and public authorities when it comes to protecting and managing that information, many companies have decided that AI is one of the only ways to keep up with increasingly sophisticated criminals. Today, for example, social media companies are expected to uncover and remove terrorist recruitment videos and messages almost instantly. In time, AI-powered crime-fighting tools could become a requirement for large businesses, in part because there will be no other way to rapidly detect and interpret patterns across billions of pieces of data.

But determining whether AI crime-fighting solutions are a good strategic fit for a company depends on whether the benefits outweigh the risks that accompany them. One such risk is that biased conclusions can be drawn from AI based on factors like ethnicity, gender, and age. Companies can also experience backlash from customers who worry that their data will be misused or exploited by even more data-intensive surveillance of their records, transactions, and communications – especially if those insights are shared with the government. Recently, for example, a European bank was forced to backtrack on its plan to ask customers for permission to monitor their social media accounts as part of its mortgage application process, after a public outcry over its "Big Brother" tactics.

So how are leading-edge companies evaluating the benefits and risks of rapidly evolving AI crime-fighting and risk management? Below, we explain some of the steps they're taking.

Determining whether AI crime-fighting solutions are a good strategic fit for a company depends on whether the benefits outweigh the risks that accompany them

EVALUATING THE STRATEGIC FIT

Before embarking on an AI risk management initiative, managers must first understand where machine learning is already making a big difference. Banks, for example, are

halting financial crimes much more quickly and cheaply than they used to by using AI for automating processes and conducting multilayered "deep learning" analyses. Even though banks now file 20 times more suspicious activity reports linked to money laundering than they did in 2012, AI tools have permitted them to shrink the armies of people they employ to evaluate alerts for suspicious activities. That's because their false alerts have fallen by as much as half thanks to AI, and because many banks are now able to automate routine human legwork in document evaluation. For example, using artificial intelligence, Paypal has also cut its false alerts in half. And Royal Bank of Scotland prevented losses of over $9 million to customers after conducting a year-long pilot with Vocalink Analytics, a payments business, to use AI to scan small business transactions for fake invoices.

50 percent

How much banks have reduced their false suspicious activity alerts thanks to AI

AI tools also allow companies to surface suspicious patterns or relationships invisible even to experts. For instance, artificial neural networks can enable employees to predict the next moves of even unidentified criminals who have figured out ways around alert triggers in binary rules-based security systems. These artificial neural networks link millions of data points from seemingly unrelated databases, containing everything from social media posts to internet protocol addresses used on airport Wi-Fi networks to real estate holdings or tax returns, and identify patterns.

The next step in assessing the wisdom of launching an AI risk-management program is for companies to evaluate to what extent customers and government authorities will expect them to be ahead of the curve. Even if it does not become a regulatory or legal obligation, companies might find it advantageous to play a leading role in the use of advanced analytics so they can take part in setting industrywide standards. They can help ensure that industry participants, regulators, technology innovators, and customers are kept safe, without trampling on people's privacy and human rights.

Finally, managers need to determine whether it makes more sense to build or buy the type of AI solution that meets their needs. To reach this decision, managers should seek proven use cases in which AI is already achieving what they hope to accomplish. Then, they should decide which vendor to work with, based on their ability to handle machine learning that addresses the type of problem faced by the managers' company with the level of quality that will satisfy regulators. If a company is likely to face more complicated or rapidly evolving crimes, however, it might require more sophisticated and customized modeling. In that case, it is usually more beneficial to develop a machine-learning solution in-house. This is especially true if externally provided solutions are expensive, provide a low degree of certainty in their results, or cannot be adapted quickly enough to keep up with a rapidly evolving marketplace.

WHAT'S NEXT?

THE RISE OF PUBLIC-PRIVATE PARTNERSHIPS IN AI CRIME PREVENTION

Companies and law enforcement agencies have been experimenting separately with using artificial intelligence to improve their ability to detect and prevent crime. Now, they are increasingly working together – developing shared data platforms, reporting protocols, and feedback loops.

Public-private partnerships to fight crime will become increasingly common. Financial institutions, financial intelligence units, and law enforcement are starting to establish public-private partnerships to share data and use AI to detect crime in certain jurisdictions. For instance, in the United Kingdom, the National Crime Agency is working closely with UK Finance to use AI in order to better identify not only financial and economic crime but also improve their ability to use financial information to detect other types of crimes like human trafficking and counterfeiting. Authorities are also exploring ways to increase the exchange of information and intelligence between the public and private sectors.

As organized crime and criminals become more sophisticated and the amount of data available to the private sector continues to increase exponentially, companies and law enforcement will enter even more public-private partnerships to leverage their wealth of data and detect potential criminal activities even more efficiently.

WHERE AI WILL BE USED TO DETECT CRIMES IN THE FUTURE

Today, AI is most commonly used to detect crimes such as fraud and money laundering. But in the future, it will likely become commonly used in other industries as well. Below are three areas where we see AI being used to prevent:

1. Transportation of illegal goods. With AI, express delivery companies can assess the likelihood that parcels contain illegal goods, like narcotics, and report them to the relevant authorities.

2. Terrorist activities. Retailers and pharmacies could use sophisticated AI tools to identify customers who purchase unusual amounts of chemicals that could be used as precursors to terrorist activities.

3. Human trafficking. Shipping companies can use their data and AI capabilities to identify the containers that are most likely to be used for human trafficking and thus save lives.

ASSESSING AND MITIGATING INTERNAL RISKS

As managers examine how AI can assist them in identifying criminal activities, they should also consider how it fits in with their broader AI strategy. AI risk management and crime detection should not be conducted in isolation. Back-testing against simpler models can help banks limit the impact of potentially inexplicable conclusions drawn by artificial intelligence, especially if there is an unknown event for which the model has not been trained. For example, banks use artificial intelligence to monitor transactions and reduce the number of false alerts they receive on potential rogue transactions, such as money that's being laundered for criminal purposes. These are back-tested against simpler rules-based models to identify potential outliers. An AI model may, for example, mistakenly overlook a large money laundering transaction that would normally trigger an alert in a rules-based system if it determines, based on biased data, that large transactions made by customers who reside in wealthy neighborhoods do not merit as much attention. Using this approach enables companies to design more transparent machine-learning models, even if that means they operate within more explicit bounds.

Companies should also prepare to adjust their risk management processes to systematically counter self-learning, AI-powered models that can develop biases as they constantly recalibrate. Banks, for example, should frequently test and verify a random subset of their money laundering and fraud analyses to ensure that AI-driven systems are not unfairly penalizing any particular group.

Most of all, managers should assess whether their company's data analytics are sufficient to handle complex AI tools. If not, they need to develop data analytics capabilities in-house to reach a critical mass of automated processes and structured analytics.

UNDERSTANDING AND PREPARING FOR EXTERNAL RISKS

Increased use of AI tools for crime prevention could also cause external risks to cascade in unexpected ways. A company could lose its credibility with the public, regulators, and other stakeholders in myriad ways – for example, if there are false alerts that mistakenly identify people as "suspicious" or "criminal" due to a racial bias unintentionally built into the system. Or, at the other end of the spectrum, they could suffer reputational damage if they miss criminal activities, like drug trafficking conducted by their clients or funds channeled from sanctioned countries such as Iran. Criminals could resort to more extreme, and potentially violent, measures to outmaneuver AI. Customers could flee to less closely monitored entities outside of regulated industries. A moral hazard could even develop if employees become too reliant on AI crime-fighting tools to catch criminals for them. Employees could feasibly develop a false sense of comfort, and then stop regularly checking the outputs and miss obvious cases.

To prevent this from happening, companies need to create and test a variety of scenarios of cascading events resulting from AI-driven tools used to track criminal activities. To outsmart money launderers, for example, banks should conduct "war games" with ex-prosecutors and investigators to discover how they would beat their system.

With results produced through scenario analysis, managers can then help senior executives and board members decide how comfortable they are with using AI crime-fighting. They can also develop crisis management playbooks containing internal and external communication strategies so they can react swiftly when things (inevitably) go wrong.

By using AI, companies can identify areas of potential crimes such as fraud, money laundering, and terrorist financing – in addition to more mundane crimes such as employee theft, cyber fraud, and fake invoices – to help public agencies with prosecuting these offenses much more effectively and efficiently. But with these benefits come risks that should be openly, honestly, and transparently assessed to determine whether using AI in this way is a strategic fit. It will not be easy. But clear communication with regulators and customers will allow companies to rise to the challenge when things go wrong. AI will eventually have a hugely positive impact on reducing crime in the world – as long as it is managed well.

Lisa Quest is a London-based partner in Oliver Wyman's Public Policy and Organizational Effectiveness practices.
Anthony Charrie is a principal in Oliver Wyman's Public Policy practice in Europe.
Subas Roy is a London-based partner in Oliver Wyman's Digital, Technology, Operations & Analytics practice.

This article first appeared in Harvard Business Review on August 9, 2018.