The Dark Side of AI and HR Departments

The topic of artificial intelligence (AI) is nearly inescapable and hotly debated. Everything from entertainment and art to business and healthcare has been impacted by the evolving technology. While there are many potential positive applications, there are also many reasons to approach the technology cautiously. Just as the internet opened up a whole new world of possibilities – you could easily access an entire library's worth of information at the press of a button – it also created a new avenue for criminals to operate. Now, criminals can use the dark web for unsavory activities or to target unsuspecting victims through cybercrime.

While we are certainly not inclined to be conspiracy theorists, there are realities with any new technology that companies should also consider, including the potential pitfalls AI can present. So, while using the technology may not be a bad idea, AI tools should be carefully researched and evaluated before making any

decision. Let's dive into some of the things you may not have considered when evaluating AI for your organization's HR department.

Responding to Increased Government Oversight

The HR regulatory landscape is already complex and constantly changing, making it difficult for HR departments to keep up. AI presents a new set of challenges. A very likely eventuality is that the US Department of Labor (DOL) develops its own AI that can assess a company's human resources information system (HRIS). Currently, the DOL relies on manually generated reports. However, with the emergence of DOL AI technology – which could happen within the next three to five years – new laws could make it possible for this technology to automatically connect and integrate with your HRIS. With this technology, the DOL would be able to see within milliseconds whether or not a company has discriminatory hiring practices.

For example, if a company is hiring for a position, the DOL would be able to assess the information provided by applicants and combine that with government data to know the gender, age, and race of the applicants. The DOL would also be able to leverage publicly available data found on platforms such as LinkedIn as well. For any data that is not publicly available, the DOL would be able to work with the Department of Justice to obtain a court order to obtain the data.

Another very real scenario in the not-so-distant future would be AI accessing your HRIS system and looking at all payroll, HR, and benefits data which would be combined with data from other third-party data providers to see if you were ACA compliant and how much the fine would be. All in milliseconds. AI could generate trillions of dollars in revenues (fines and penalties) for the government. Whatever AI technology is developed by the government will likely be light years ahead of commercially available tools, so again, while it's not a bad idea, AI will make it easier for the government to identify non-compliance than ever before. Thus, companies will need to be extremely proactive regarding compliance moving forward.

Navigating New Data Security Challenges

With the immense amounts of data AI tools will have access to, they'll know everything about your company and its employees. Some of this data, like knowing where employees live or go to the doctors, can make it possible to provide tailored benefits, thus making benefits administration more personalized. Even so, it poses security risks. If a hacker were to hack into the AI tool, they could steal all this employee data. Additionally, the AI tool developer may be inclined to sell data for profit, which could pose another threat.

If an AI technology's database is breached, it could be easy for cybercriminals to uncover not only where someone lives and their bank accounts, but also what medical conditions they may have, where they go to the doctor, what prescriptions they have, the names and date of births for all their children, plus a lot more. Someone's entire life data could be stolen and used to fraudulently open bank accounts, change their W-2s and have a refund set to an offshore account and let them deal with the IRS, or cancel lifesaving prescriptions for anyone in their family. Other AI tools could be employed by hackers to identify what credit cards have minimal background checks. All data processed by an AI tool needs to be housed somewhere, and when relying on a third-party provider, data can be more vulnerable to breaches or attacks.

Ensuring Technology is Up-to-Date

Typically, systems and software require periodic updates to ensure they are bug-free, introduce new features, and reinforce security measures. If any technology becomes outdated, it can pose security threats and other challenges. With AI, this could mean detrimental inaccuracies.

For example, think of a police department's speed radar detector. If an officer issued a speeding ticket and the recipient fought the ticket in court, demanding proof of the radar's recent calibration, the judge could throw out the ticket if the police department failed to calibrate the machine recently. An all-to-common scenario faced by police departments across the country, departments reassessed their policies around calibration.

We could see parallel scenarios within the HR department arise as the use of AI technologies continues to proliferate. If the Department of Labor were to bring in the hypothetical AI discussed earlier to assess a company for violations such as discriminatory hiring practices or inaccurate wages per hour, the company may also seek to fight back if it believes the AI assessment is inaccurate. This highlights that if a company is looking to use AI, it should have a well-defined plan as to who is responsible for ensuring that the technology is up-to-date and when.

How Should HR Departments Respond?

Rather than just assuming it's a bad idea, AI tools should be carefully researched to understand the advantages and disadvantages before implementation. Fundamentally, AI is no different than any other transformative technology. The difference between successful and unsuccessful implementation is how the technology is leveraged. HR departments should seek to partner with an HR outsourcing company, like Corban OneSource, that is truly embracing AI. For example, if an AI platform emerges that understands every jurisdiction's employment and tax law compliance requirements, HR departments will still need someone who can deploy the changes necessary to get and stay compliant. A good HRO will keep its finger on the pulse of these new technological developments, so it can be a trusted partner for companies looking to implement the newest technology to proactively address their compliance needs.

For many people, a major concern around AI is the potential to eliminate jobs. While it does have the potential to streamline processes for recruitment or talent acquisition, humans will be a necessary component. Humans will be needed to deploy the technology and ensure it is up-to-date and meets the needs of the company. With AI, compliance is likely to get much more complex, so having the right team of humans to interpret and understand new compliance measures will be essential for success as well.

AI is a complex and continually evolving subject that needs to be carefully watched to be understood. As with many great technologies, there are many positive

attributes that create new efficiencies. While it isn't a bad idea, AI must be strategically and carefully evaluated to understand where the technology fits within the HR department.

Fortunately, relying on an HRO like Corban OneSource can make the process easier for companies that have between 75 and 6,000 employees. Our US-based team will work with you to ensure you have the right AI tools to support HR processes while also remaining compliant with all applicable regulations and protecting sensitive data. Contact us today to explore how we can help you implement the latest AI technology while remaining compliant and securing your data appropriately.