Data Security

Cyber-Risks in Emerging Technologies: Preparing for the Use of AI

by **Jordan L. Fischer** | *Fischer Law, LLC*

Artificial intelligence (AI) has rapidly evolved from a futuristic concept to an integral part of the operations of many businesses. Its potential to enhance productivity, automate tasks and derive valuable insights from data is undeniable. However, with the integration of AI into various aspects of business, cyber-risks cannot be overlooked and need to be identified and understood by employers at all levels.

As businesses embrace AI technologies, they must also prioritize cybersecurity measures to safeguard sensitive data and operations. This is especially relevant for employee benefit plans, which process large amounts of data, making AI both intriguing and potentially fraught with risk for both the employer and the individuals whose data is impacted.

This article will explore how AI is changing the workforce, especially in the context of employee benefit plan administration, as well as some of the key cyber-risks associated with the use of AI. It will then discuss strategies for preparing both employees and employers to mitigate these risks effectively.

AI Is Rapidly Changing the Way We Work and Do Business

A recent article by McKinsey and Company defines AI as “the broad field of developing machines that can replicate human behavior, including tasks related to perceiving, reasoning, learning and problem-solving.”[1] The integration of AI into various aspects of business operations creates changes that have significant implications for the workforce. This is especially heightened with the use of generative AI (tools such as ChatGPT), which can create outputs (images, text, etc.), providing increased capacity across a variety of functions. Whether an employer is using AI or generative AI, key changes for business operations include the automation of routine tasks, the augmentation of human capabilities, the creation of new jobs and the changing of the skills needed to

AT A GLANCE

- Key developments for business operations with the use of artificial intelligence (AI) include the automation of routine tasks, the augmentation of human capabilities, the creation of new jobs and the changing of the skills needed to operate in an AI-driven business world.
- The high volume and sensitive nature of data involved in the use of AI create privacy and cyber-risks for businesses and employee benefit plans in particular. Benefit plans should select AI tools that have numerous opportunities for oversight and checks to make sure that decisions are not made that negatively impact plan members and result in a violation of employer fiduciary duties.
- Key steps to secure businesses and employee benefit plans for the future of AI include carefully negotiating contracts with AI providers, being judicious when deciding what information is ingested into an AI tool, and creating regular opportunities for human oversight and checks on the tool.

operate in an AI-driven business world. Each is addressed below.

Automation of Routine Tasks

One of the most immediate effects of AI on the workforce is the automation of repetitive and routine tasks. AI-powered software and robotics can efficiently perform tasks that are rule-based and predictable, such as data entry, document processing and customer support. As a result, jobs that primarily involve such tasks may be replaced or augmented by AI systems, leading to shifts in job roles and skill demands. For employee benefits administration, the ability to automate certain tasks could create opportunities to leverage resources elsewhere or to find cost savings. For example, routine data analysis and auditing that a benefit plan may be required to do can now be significantly addressed via AI tools. In addition, fraud prevention can be significantly improved by leveraging AI to look for suspicious patterns. While these examples still would require some human oversight, it would significantly decrease the manual hours needed to conduct these reviews.

Augmentation of Human Capabilities

While AI may automate certain tasks, it also has the potential to augment human capabilities and enhance productivity, such as by creating more effective use of employee time. AI-powered tools can assist workers by providing valuable insights, automating decision-making processes and enabling more efficient resource allocation. For example, AI-driven analytics platforms can help professionals in various fields—such as finance, marketing and health care—make data-driven decisions and predictions.

Creation of New Job Roles

The adoption of AI often leads to the creation of new job roles that require specialized skills in AI development, data science, machine learning and cybersecurity. Organizations need professionals who can design, develop, implement and maintain AI systems as well as ensure their security and ethical use. Even just understanding the AI tool and helping other employees use it in their day-to-day job tasks is itself a need for many organizations. Job titles such as AI specialists, data engineers, machine learning engineers and AI ethicists are becoming increasingly prevalent in response to the growing demand for AI expertise.

Reskilling and Upskilling Needs

The integration of AI into the workforce necessitates ongoing reskilling and upskilling initiatives to ensure that employees have the essential competencies to work alongside AI technologies effectively. Workers may need to acquire new skills in areas such as data analysis, programming, digital literacy, critical thinking and problem solving to remain relevant in the AI-driven economy. Employers play a crucial role in providing training opportunities and fostering a culture of continuous learning within their organizations.

While AI automation may streamline processes and improve efficiency as it changes the workforce, it also necessitates careful consideration of ethical and social implications. By embracing these changes and investing in workforce development, employers can harness the transformative potential of AI while ensuring the well-being and productivity of their employees. However, all the opportunities that AI creates in the workforce come with corresponding risks that should be understood and addressed before fully embracing AI.

Understanding the Privacy and Cyber-Risks

The risks presented by AI range from legal compliance risks to operational risks created by any given AI tool. Each organization should weigh the advantages of using an AI tool against the potential costs before diving headlong into this new technology.

One of the biggest legal risks in the use of AI tools stems from potential data privacy compliance challenges. AI systems rely heavily on data—often large volumes of personal or sensitive information. With evolving U.S. and global data privacy regulations, this personal information is potentially subject to legal requirements, including data rights as well as notice and consent obligations prior to its usage. Regulators are still grappling with how to apply these data protection regulations in the AI context, but for now, businesses should use caution whenever an AI tool could ingest and leverage personal information.

Privacy concerns are especially relevant in the context of more sensitive information, such as employee information and health information. Because this data presents a heightened risk to the individual, and (in the context of health information) is often easily identifiable to the individual, the use of AI to process or manipulate this information should be limited and highly reviewed.

Second, because of the high volume of data within these AI systems, AI applications become lucrative targets for cybercriminals seeking to steal or manipulate data for malicious purposes. In addition to personal information, data may also include proprietary information about a business' practices, technology or other insights. AI is not unique and presents the same cybersecurity concerns as any other tool—Wherever there is potentially high-value data, attackers will attempt to breach those systems and gain access to that information. Ensuring that it is well-protected and remaining vigilant in those protections is key. This includes having strong access controls, requiring complex passwords and multifactor authentication for all accounts, and training users on how to securely use these tools.

Third, because AI tools are so heavily reliant on the data that they ingest, they are also susceptible to adversarial attacks when bad actors manipulate them, feeding them misleading or malicious data. These attacks can deceive AI algorithms, leading to incorrect decisions or behaviors. Adversarial attacks pose a serious threat, especially in critical applications such as autonomous vehicles, medical diagnostics or financial trading algorithms.

Finally, and building again on the AI tool's heavy reliance on the data it ingests, AI algorithms are susceptible to bias, which can result in unfair or discriminatory outcomes and create a compliance risk, particularly in areas like hiring or lending. Bias can occur if only a certain subset of data is used to train the model, meaning that other perspectives, images, etc., are not taken into consideration. Biased AI models not only undermine ethical principles but also expose businesses to legal liabilities and reputational risks. The technology driving the AI models is such a black box, even for the technologists who are well-versed in these tools, that addressing bias and ensuring fairness in AI systems requires careful attention to data selection, algorithm design and ongoing monitoring.

For the administration of employee benefits, the privacy and cyber-risks are especially relevant because of the high amounts of sensitive personal information handled by employees. It is even more important that benefit plans select AI tools that have numerous opportunities for oversight and checks to make sure that decisions do not negatively impact plan members and result in a violation of employer fiduciary duties.

Preparing the Workforce

AI is increasingly being used across all industries to help address a variety of business concerns. Everyone is likely encountering AI on a daily basis, whether they know it or not. Therefore, it is important to prepare employees for these tools and how to responsibly leverage them within their jobs.

The first step is educating and training employees on AI. When AI first became mainstream, many businesses feared its use and banned employees from using these tools. However, this approach is changing as businesses recognize AI's pervasiveness. Embracing the technology—but with an informed workforce—is likely a better, more sustainable approach. This requires businesses to invest in comprehensive training programs to educate the workforce about both the opportunities and risks associated with these AI technologies. Training can include the types of data that should be used with AI and, more importantly, the types of data that should not be used in AI. In addition, users should be aware that human oversight should be included to confirm that outputs are accurate and can be relied upon.

Second, creating opportunities for cross-collaboration is never more important than when a business is using AI tools. This includes facilitating collaboration between cybersecurity teams, AI developers, data scientists and other relevant stakeholders. Employers should encourage open communication channels to ensure that security considerations are integrated into the development and deployment of AI solutions from the outset. A good example is engaging with security teams early on in the selection and implementation of a new AI tool, allowing security to be considered prior to the tool's implementation.

Finally, encouraging employees to ask questions, become informed and be curious about AI is also important. AI is not going away and will only become more integrated across operations and other tools that an employer is already using.

International Society of Certified Employee Benefit Specialists

Reprinted from the Third Quarter 2024 issue of *BENEFITS QUARTERLY*, published by the International Society of Certified Employee Benefit Specialists. With the exception of official Society announcements, the opinions given in articles are those of the authors. The International Society of Certified Employee Benefit Specialists disclaims responsibility for views expressed and statements made in articles published. No further transmission or electronic distribution of this material is permitted without permission. Subscription information can be found at iscebs.org.

Urging employees to better understand when AI is leveraged and what that means for the employer will be a critical step in identifying AI risks and mitigating them in the long run. To help facilitate these conversations, employers should develop an AI policy that provides guardrails for the use of AI and details how employees can raise questions or concerns with using AI.

Securing the Business and Benefit Plan for the Future of AI

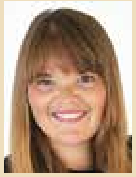
While businesses need to prepare for the integration of AI into most, if not all, of their operations, they can take certain key steps when moving forward with any AI tool to help secure themselves and their benefit plans from a risk perspective.

1. **Carefully negotiate contracts with AI providers.** These contracts lay out key terms for data usage, indemnification and liabilities. Making sure that the employer or benefit plan has adequate contractual protections, in the event that the AI tool causes a harm to employees or creates other risks, is key to minimizing the risk in using the tool. This is especially relevant when dealing with protected health information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA). Increasingly, covered entities are restricting the use of AI tools in the processing of PHI and requiring business associates to proactively seek consent prior to the use of any AI. When negotiating a business associate agreement (BAA), it is important to flag AI as a higher risk and place parameters around its use.
2. **Judiciously consider what personal information is ingested into the tool and the privacy and security controls implemented to reduce risk**. Deploying comprehensive security controls to protect AI systems and data assets from unauthorized access, manipulation and theft is critical since these tools are often seen as a high-value target by threat actors. AI tools should include encryption, access controls, authentication mechanisms and regular security assessments to identify vulnerabilities. In addition, it's key to have privacy controls that inform users of the data that can be input into the AI tool and, more importantly, the data that cannot be put into the AI tool.
3. **Create regular opportunities for human oversight and checks on the tool**. Running these tools without any checks on how they are used and the output that is generated can create costly outcomes for plan sponsors. Employers and benefit plan sponsors should establish processes for reviewing, assessing and confirming that AI tools continue to function as intended and that plan members and employees are adequately protected from adverse impacts from the use of these tools.

Conclusion

While the adoption of AI technologies offers numerous benefits for employers, it also introduces inherent privacy, general business and cyber-risks that must be addressed proactively. By understanding these AI tools, educating the workforce, and implementing appropriate security and privacy controls, employers can mitigate the potential threats associated with the use of AI. Ultimately, not only will a proactive approach to AI protect the employee benefit plan and align with the plan sponsor's fiduciary duties, it will foster trust and confidence among plan members and stakeholders in an increasingly AI-driven world. BQ

AUTHOR



Jordan L. Fischer is the founder and partner at Fischer Law, LLC, law firm in Philadelphia, Pennsylvania. She is a data privacy and cybersecurity attorney with extensive experience in the global intersection of law and technology. Fischer is a Certified Information Privacy Professional for Europe (CIPP/E) and a Certified Information Privacy Professional for the United States (CIPP/US), as well as a Certified Information Privacy Manager (CIPM), as certified by the International Association of Privacy Professionals. She is a lecturer at the University of California, Berkeley School of Information.

Endnote

[1] McKinsey & Company. "What is AI (artificial intelligence)?" www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai.