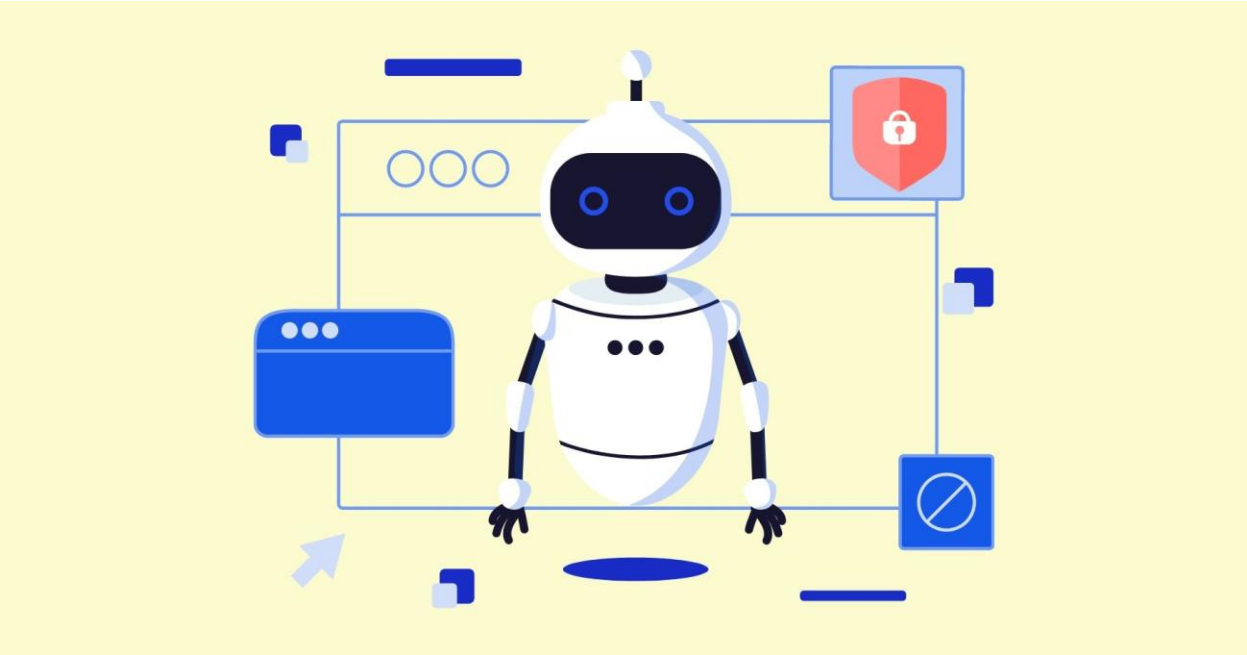
How to Manage Evolving Third-Party AI Risks

By: Christine Kitamura on October 17 2023

7 min read



Despite the prevalence of artificial intelligence (AI) in today's world, it seems as though humans have historically been wary about it. The sci-fi genre is filled with unnerving stories about AI, such as the disobedient computer system in 2001: A Space Odyssey or The Terminator sent to eradicate the human race.

Though these stories might be exaggerated, it's worth noting that AI does have some real-world risks that need to be managed, such as privacy, cybersecurity, and ethics. If your third-party vendors have started to implement AI technology, it's important to **understand how to manage these risks**.

In this blog, we've outlined the primary goal of managing each risk, and some common risk factors that should be considered. We also provided a few helpful tips to include in your **third-party risk management (TPRM)** program.

The Privacy Risks of Third-Party Artificial Intelligence

Data privacy continues to be a hot topic for information security leaders, especially as new state laws and regulations seem to emerge every few months. When a third-party vendor uses AI and has access to **personally identifiable information (PII)**, these are just some of the specific risk factors that you'll need to consider:

- **Misuse of data:** Artificial intelligence relies on vast amounts of data. It should only be used in a way that complies with regulations and your organization's standards. There's a risk that a third party could intentionally or unintentionally misuse your data. For example, they may use your data for targeted advertising, training their own AI model, or they could even sell it to another company.
- **Inadequate data anonymization:** This process is intended to keep data sources anonymous by removing certain identifiers. For example, your third-party vendor might store Social Security numbers and account numbers, but anonymization would prevent that data from being associated with an individual. AI begins with humans and is therefore not infallible, so there's a possibility of poor data anonymization.
- **Non-compliance with privacy regulations:** A third-party vendor that stores or transmits data through an AI system can expose you to **compliance risk**, which can result in financial loss through regulatory fines and litigation fees. For example, if your third party shares PII with a subcontractor (i.e., your fourth party) in a location with different privacy laws, it could result in a compliance issue if your third party is unaware of these regulations.

How to Manage Third-Party Artificial Intelligence Privacy Risk

A good strategy to manage a third-party vendor's privacy risk includes minimization, mitigation, monitoring, and maintenance. Below are brief descriptions of each component:

1. **Minimization** – Limit the amount of data you share with your third-party vendor to only what is necessary. If they don't need certain data to perform an activity, they shouldn't have access to it.
2. **Mitigation** – Verify that your third party has controls in place to close any gaps that exist between their privacy practices and your requirements. Mitigating controls might include things like data pseudonymization, anonymization, and encryption. You should also outline **data privacy expectations in the contract** to minimize risks.
3. **Monitoring** – Your **third-party vendor should be regularly monitored** to ensure they're following your contractual requirements about data privacy.
4. **Maintenance** – Stay updated on privacy legislation and implement any changes to your internal requirements as needed. For example, maybe your state has just amended its privacy law to expand the definition of PII. This situation should trigger

a thorough review of your third party's policies and notices to make sure that they align with this new definition.

The Cybersecurity Risks of Third-Party Artificial Intelligence

Cyberattacks and data breaches aren't new threats. However, the use of AI has brought new challenges in addressing them. Because of the newness of many of these third-party services, AI tools may not meet cybersecurity best practices.

Data stored, processed, or maintained by an AI system may be at risk due to the following factors:

- **Data and system manipulation:** Many cybercriminals steal data or corrupt it in a ransomware attack, but AI technology can introduce a different type of threat with data and system manipulation. Since data is used to train AI systems, cybercriminals can potentially manipulate that data to produce inaccurate and harmful results. For example, an AI system that predicts diagnoses using health information can create an incorrect diagnosis if that information is manipulated.
- **Automated attacks:** Because AI isn't inherently good or bad, cybercriminals can use this technology for malicious purposes, such as launching an automated phishing attack. This can create a unique dilemma of a third-party vendor's AI system being compromised by a more sophisticated AI system. This level of sophistication can make it harder to detect and prevent these cyber incidents.

How to Manage Third-Party Artificial Intelligence Cybersecurity Risk

Managing your **third-party vendor's cybersecurity risk** requires a comprehensive strategy, whether they're using AI technology or not. Here are four main components you'll want to address with your vendor:

1. **Monitor and test** – Your third-party vendor should actively monitor their cybersecurity risk to ensure that they can quickly detect and respond to any incidents that may impact your data. Penetration testing is also an important component that will help your vendor identify any gaps or weaknesses before they're exploited by attackers.
2. **Train** – Cybersecurity training is essential for any teams and individuals that have access to your data. Your vendor should provide evidence that their employees, contractors, and vendors have been properly trained in cybersecurity best practices. If your third party is using AI, you should also verify that employees have been educated on the best AI practices. Check if your third-party vendor has limits on employee use of tools like generative AI.

3. **Data breach notification** – It's important to remember that vendor data breaches aren't 100% preventable. However, including **data breach notification requirements in your vendor contract** will help keep you in compliance and set expectations for what your vendor needs to do when an incident occurs with an AI system. Consider whether you want to implement more rigid requirements such as a shorter timeline for notification or more frequent security testing.
4. **Due diligence** – The due diligence process should engage qualified subject matter experts (SMEs) who are knowledgeable in AI risk. These SMEs can review the vendor's controls and determine whether they're effective in protecting against cyber incidents.

The Ethical Risks of Third-Party Artificial Intelligence

The ethical risk of AI is perhaps the most challenging to address because opinions vary widely on what is morally acceptable and not. A lack of comprehensive federal legislation can also add to the uncertainty over how to manage ethical risk.

Here are some examples of ethical risk in AI:

- **Bias and fairness:** AI systems can intentionally or unintentionally be programmed with bias, which can create disadvantages to certain individuals or groups. One real-life example involves AI use in Amazon's recruitment. Their AI model was trained on data that came mostly from male resumes, which ultimately discriminated against female applicants.

- **Lack of transparency:** When AI models lack transparency, it can create ethical concerns regarding their advice or decision-making. For instance, if a user is unaware of why a third-party AI system denied a loan application, is it ethical to continue using it?
- **Environmental impact:** In recent years, there's been a growing focus on **environmental, social, and governance (ESG)** issues, and regulators are discussing mandatory disclosures and reporting. It's natural to wonder about the impact of AI on these issues. Typically, AI systems need significant energy and financial resources for training, which contributes to the debate about their effect on the environment.

How to Manage Third-Party Artificial Intelligence Ethical Risk

Ethics can generally be a "grey" area so every organization will have to decide on a strategy that works best for them. Here are some next steps you may want to consider within your own third-party risk management program:

1. **Continue learning** – AI is evolving quickly, but it's important to continue learning about the basics and understand how your third-party vendors are using this technology. The more you learn about AI and its applications, the better prepared you'll be to identify ethical risks.
2. **Define your standards** – It's important to have clear ethical guidelines and oversight in place to manage the potential risks of AI and ensure it's used in an ethical and responsible manner. You can't expect your third-party vendors to follow standards that don't exist, so consider developing your own code of conduct or **governance documentation** that specifies what your organization considers ethical.
3. **Make sure AI decisions aren't made in isolation** – To manage ethical risk, it's crucial to involve a diverse group of voices and perspectives when making decisions about AI. With this approach, your organization can better understand the potential consequences of AI and make more ethical and responsible decisions, which will benefit your organization and its customers.

AI has the potential to create significant benefits across all industries. It's essential, however, to address the unique privacy, cybersecurity, and ethical risks associated with AI to make sure your third-party vendors can use it safely and effectively. As AI use continues to be more widespread, third-party risk management teams will be integral to protecting their organizations and customers against these AI risks.